

This page Is Inserted by IFW Operations
And is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of
The original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
Please do not report the images to the
Image Problem Mailbox.**

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-327147

(43) 公開日 平成10年(1998)12月8日

(51) Int.Cl. ⁶	識別記号	F I
H 0 4 L 9/32		H 0 4 L 9/00 6 7 5 D
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00 6 4 0 B
	6 6 0	6 6 0 B
		6 6 0 A
H 0 4 L 9/10		H 0 4 L 9/00 6 2 1 Z
審査請求 未請求 請求項の数30 F D (全 54 頁)		

(21) 出願番号 特願平9-147319

(22) 出願日 平成9年(1997)5月21日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 洲崎 誠一

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72) 発明者 水野 康彦

神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所ビジネスシステム開発センタ内

(74) 代理人 弁理士 矢島 保夫

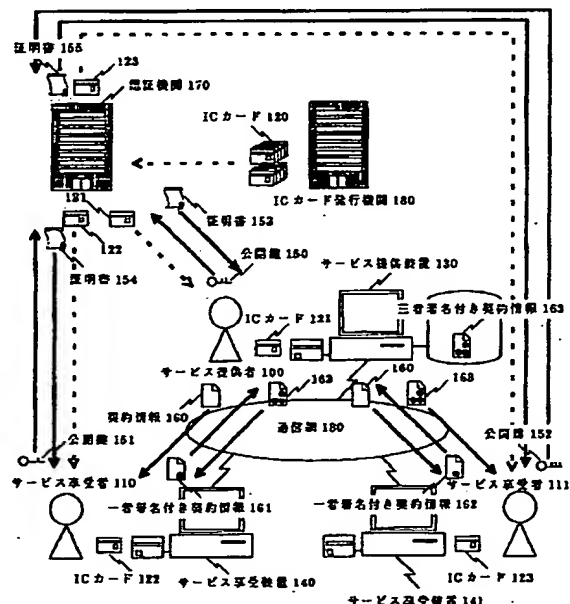
最終頁に続く

(54) 【発明の名称】 電子認証公証方法およびシステム

(57) 【要約】 (修正有)

【課題】 オープンなネットワーク環境において電子商取引に必要な認証・公証サービスを実現する。

【解決手段】 サービス提供装置130から契約内容を含む契約情報を契約者である各サービス享受者110、111のサービス享受装置140、141に送信し、契約情報を受信した各サービス享受装置で契約情報にサービス享受者の署名を付けた一者署名付き契約情報161、162を作成してサービス提供装置に送信する。サービス提供装置では各サービス享受装置から送信された一者署名付き契約情報を受信し、まとめて一つの文書にし、サービス提供者の署名を付けたサービス提供者署名付き契約情報163を作成し、保管するとともに各サービス享受装置に送信する。



【特許請求の範囲】

【請求項1】公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを受受する複数のサービス享受者がそれぞれ使用する複数のサービス享受装置とが、ネットワークを介して相互に接続されているシステムに適用する電子認証公証方法であって、前記サービス提供装置から、契約内容を含む契約情報を、契約者である各サービス享受者のサービス享受装置に、それぞれ送信するステップと、該契約情報を受信した各サービス享受装置で、該契約情報にサービス享受者の署名を付けた一者署名付き契約情報を作成し、前記サービス提供装置に送信するステップと、前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報をまとめて一つの文書にするとともに、該文書にサービス提供者の署名を付けたサービス提供者署名付き契約情報を作成するステップと、前記サービス提供装置で、作成したサービス提供者署名付き契約情報を保管するステップと、前記サービス提供者署名付き契約情報を、前記サービス提供装置から前記各サービス享受装置に送信するステップとを備えたことを特徴とする電子認証公証方法。

【請求項2】公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを受受する複数のサービス享受者が使用する複数のサービス享受装置と、前記サービス提供者および各サービス享受者の公開鍵が確かにその者の公開鍵であることを保証する証明書を発行する認証機関の端末装置とが、ネットワークを介して相互に接続されているシステムに適用する電子認証公証方法であって、前記サービス提供装置で、前記サービス提供者の公開鍵と秘密鍵とを生成するステップと、前記各サービス享受装置で、それぞれ、前記各サービス享受者の公開鍵と秘密鍵とを生成するステップと、前記サービス提供装置および各サービス享受装置から、生成した公開鍵を前記認証機関の端末装置に送信するステップと、前記認証機関の端末装置で、受信した公開鍵ごとに、その公開鍵に対応する証明書を作成し、それぞれ対応する前記サービス提供装置および各サービス享受装置に送信するステップと、前記サービス提供装置および各サービス享受装置で、前記証明書をそれぞれ受信するステップと、前記各サービス享受装置から、それぞれ、契約内容その他の契約に係る各種の情報を前記サービス提供装置に送信するステップと、前記サービス提供装置において、前記各サービス享受装置からそれぞれ送られてくる契約に係る各種の情報をま

とめて契約内容を含む契約情報を作成し、前記各サービス享受装置にそれぞれ送信するステップと、前記各サービス享受装置で、それぞれ、受信した契約情報にサービス享受者の証明書を含む付属情報を所定の順序で連結したデータを作成し、該連結したデータを所定の一方方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス享受者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせて一者署名付き契約情報を作成し、該一者署名付き契約情報を前記サービス提供装置に送信するステップと、前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報から契約情報並びに各サービス享受者が付加した付属情報および署名を取り出し、取り出した情報とサービス提供者の証明書を含む付属情報とを所定の順序で連結したデータを作成し、該連結したデータを所定の一方方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス提供者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせてサービス提供者署名付き契約情報を作成するステップと、前記サービス提供装置で、作成したサービス提供者署名付き契約情報を保管するステップと、前記サービス提供者署名付き契約情報を、前記サービス提供装置から前記各サービス享受装置に送信するステップとを備えたことを特徴とする電子認証公証方法。

【請求項3】前記ネットワークを介したサービス提供者およびサービス享受者と認証機関との間の通信は、認証機関の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用して暗号通信により行なう請求項2に記載の電子認証公証方法。

【請求項4】前記ネットワークを介したサービス提供者とサービス享受者との間の通信は、互いの証明書を交換し、サービス提供者の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用して暗号通信により行なう請求項1または2の何れか1つに記載の電子認証公証方法。

【請求項5】前記サービス提供者および各サービス享受者には、前記認証機関の公開鍵である認証機関証明書が格納されている、前記サービス提供装置およびサービス享受装置に着脱可能な、記憶媒体が、あらかじめ配布されており、前記サービス提供者および各サービス享受者の公開鍵および秘密鍵、並びに、前記認証機関が発行した証明書は、該記憶媒体に格納される請求項1または2の何れか1つに記載の電子認証公証方法。

【請求項6】前記着脱可能な記憶媒体が、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するデジタル署名生成プログラム、並びにそれらのプログラムを実

行して暗号鍵生成や署名生成を実行する処理装置を備えたICカードであり、

前記サービス提供者および各サービス享受者は、該ICカードを用いて、秘密鍵と公開鍵の生成、および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ICカードに格納する請求項5に記載の電子認証公証方法。

【請求項7】前記着脱可能な記憶媒体には、当該記憶媒体の正当な使用者のパスワードで暗号化された暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書、並びに該パスワードをチェックするためのパスワードチェック用データが格納され、上記暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書にアクセスする際には、使用者が入力したパスワードを上記パスワードチェック用データを用いてチェックし、正当な使用者であると確認された場合のみアクセスを許可する請求項5に記載の電子認証公証方法。

【請求項8】前記着脱可能な記憶媒体が、内蔵時計、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するデジタル署名生成プログラム、並びにそれらのプログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたICカードであり、

前記サービス提供者および各サービス享受者は、該ICカードを用いて、秘密鍵と公開鍵の生成および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ICカードに格納し、署名生成時には署名対象のデータに上記内蔵時計の日時データを付加したデータを秘密鍵で暗号化して署名生成する請求項5に記載の電子認証公証方法。

【請求項9】前記ICカードは、署名生成の直前に、時刻管理機関が送信する正確な時刻を示す標準時刻データを受信し、該標準時刻データに基づいて内蔵時計を調整する請求項8に記載の電子認証公証方法。

【請求項10】前記ICカードは無線受信装置を備え、該無線受信装置により受信した前記時刻管理機関からの標準時刻データに基づいて内蔵時計を調整する請求項9に記載の電子認証公証方法。

【請求項11】前記着脱可能な記憶媒体内の秘密鍵、公開鍵、および証明書をういて署名を行なったとき署名履歴を該記憶媒体内に記憶しておくとともに、該記憶媒体内の秘密鍵、公開鍵、および証明書が新たなデータに変更されたとき、署名履歴を参照して必要があれば、以前に使用した秘密鍵、公開鍵、および証明書を別領域に記憶しておく請求項5に記載の電子認証公証方法。

【請求項12】会員認証局の端末と、個人認証局の端末と、申込者の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、

あらかじめ、各申込者が、その申込者の公開鍵とその公

開鍵がその申込者のものであることを証明する証明書とを含むデジタルデータである個人認証書の配布を前記個人認証局から受けるステップと、

前記申込者の端末から前記会員認証局の端末に、個人認証書を添付した会員登録申込書を送信するステップと、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、

前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、

前記会員認証局の端末で、その確認結果に基づいて前記申込者の会員資格の審査を行なうステップと、

審査の結果、会員資格有りの場合は、前記会員認証局から前記申込者に暗号鍵生成プログラムを内蔵したICカードを配布するステップと、

該ICカード中で、申込者の公開鍵と秘密鍵を生成するとともに、生成した公開鍵を含む申込者に関する所定の情報を所定のフォーマットでまとめたデータである会員証を作成するステップと、

前記申込者の端末から前記会員認証局の端末に、前記会員証を送信するステップと、

前記会員認証局の端末で、前記申込者の公開鍵を含む会員証が確かにその者のものであることを証明する証明書を作成して、申込者の端末に送信するステップと、

前記申込者の端末で、受信した証明書を前記ICカードに格納するステップとを備えたことを特徴とする電子認証方法。

【請求項13】会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の抹消の申込みを送信するステップと、

前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、

前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、

前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、本人からの登録抹消依頼であることを確認した上で、会員登録の抹消を行なうステップとを備えたことを特徴とする電子認証方法。

【請求項14】会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の有効性の確認依頼を

送信するステップと、

前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、

前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、

前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、前記個人認証書と会員証で特定される会員の会員登録の有効性を確認し、その確認結果を前記会員の端末に送信するステップとを備えたことを特徴とする電子認証方法。

【請求項15】団体の構成員の端末が該団体内ネットワークを介して相互に接続され、該団体の構成員である登録責任者の端末が認証機関の端末とネットワークを介して相互に接続されているシステムにおいて、該団体の構成員の公開鍵の認証機関への登録および認証機関から証明書を発行してもらう処理を、該団体の登録責任者が代行して行なう電子認証方法であって、

公開鍵の登録を申請する構成員の端末において、その構成員が登録しようとしている公開鍵を認証機関の公開鍵で暗号化して、前記登録責任者の端末に送信するステップと、

前記登録責任者の端末において、受信した構成員の暗号化公開鍵に登録責任者のデジタル署名を付して、前記認証機関の端末に送信するステップと、

前記認証機関の端末において、前記登録責任者の端末から送信されたデジタル署名付きの暗号化公開鍵を受信し、前記登録責任者のデジタル署名を確認した後、前記認証機関の秘密鍵で該暗号化公開鍵を復号し、復号した公開鍵の証明書を作成し、該証明書を前記団体の公開鍵および／または前記構成員の公開鍵で暗号化して、前記登録責任者の端末または前記構成員の端末に送信するステップとを備えたことを特徴とする電子認証方法。

【請求項16】公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者がそれぞれ使用する複数のサービス享受装置とが、ネットワークを介して相互に接続されて構成される電子認証公証システムであって、前記サービス提供装置から、契約内容を含む契約情報を、契約者である各サービス享受者のサービス享受装置に、それぞれ送信し、

該契約情報を受信した各サービス享受装置で、該契約情報にサービス享受者の署名を付けた一者署名付き契約情報を作成して、前記サービス提供装置に送信し、前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報をまとめて一つの文書にするとともに、該文書にサービス提供者の署名を付けたサ

ービス提供者署名付き契約情報を作成し、該作成したサービス提供者署名付き契約情報を保管するとともに、前記各サービス享受装置に送信することを特徴とする電子認証公証システム。

【請求項17】公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者が使用する複数のサービス享受装置と、前記サービス提供者および各サービス享受者の公開鍵が確かにその者の公開鍵であることを保証する証明書を発行する認証機関の端末装置とが、ネットワークを介して相互に接続されて構成される電子認証公証システムであって、

前記サービス提供装置で、前記サービス提供者の公開鍵と秘密鍵とを生成し、

前記各サービス享受装置で、それぞれ、前記各サービス享受者の公開鍵と秘密鍵とを生成し、

前記サービス提供装置および各サービス享受装置から、生成した公開鍵を前記認証機関の端末装置に送信し、

前記認証機関の端末装置で、受信した公開鍵ごとに、その公開鍵に対応する証明書を作成し、それぞれ対応する前記サービス提供装置および各サービス享受装置に送信し、

前記サービス提供装置および各サービス享受装置で、前記証明書をそれぞれ受信し、

前記各サービス享受装置から、それぞれ、契約内容その他の契約に係る各種の情報を前記サービス提供装置に送信し、

前記サービス提供装置において、前記各サービス享受装置からそれぞれ送られてくる契約に係る各種の情報をまとめて契約内容を含む契約情報を作成し、前記各サービス享受装置にそれぞれ送信し、

前記各サービス享受装置で、それぞれ、受信した契約情報にサービス享受者の証明書を含む付属情報を所定の順序で連結したデータを作成し、該連結したデータを所定の一方方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス享受者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせて一者署名付き契約情報を作成し、該一者署名付き契約情報を前記サービス提供装置に送信し、

前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報から契約情報並びに各サービス享受者が付加した付属情報および署名を取り出し、取り出した情報とサービス提供者の証明書を含む付属情報とを所定の順序で連結したデータを作成し、該連結したデータを所定の一方方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス提供者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせてサービス提供者署名付き契約情報を作成し、

前記サービス提供装置で、作成したサービス提供者署名

付き契約情報を保管し、

前記サービス提供者署名付き契約情報を、前記サービス提供装置から前記各サービス享受装置に送信することを特徴とする電子認証公証システム。

【請求項18】前記ネットワークを介したサービス提供者およびサービス享受者と認証機関との間の通信は、認証機関の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なう請求項17に記載の電子認証公証システム。

【請求項19】前記ネットワークを介したサービス提供者とサービス享受者との間の通信は、互いの証明書を交換し、サービス提供者の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なう請求項16または17の何れか1つに記載の電子認証公証システム。

【請求項20】前記サービス提供者および各サービス享受者には、前記認証機関の公開鍵である認証機関証明書が格納されている、前記サービス提供装置およびサービス享受装置に着脱可能な、記憶媒体が、あらかじめ配布されており、

前記サービス提供者および各サービス享受者の公開鍵および秘密鍵、並びに、前記認証機関が発行した証明書は、該記憶媒体に格納される請求項16または17の何れか1つに記載の電子認証公証システム。

【請求項21】前記着脱可能な記憶媒体が、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するデジタル署名生成プログラム、並びにそれらのプログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたICカードであり、

前記サービス提供者および各サービス享受者は、該ICカードを用いて、秘密鍵と公開鍵の生成、および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ICカードに格納する請求項20に記載の電子認証公証システム。

【請求項22】前記着脱可能な記憶媒体には、当該記憶媒体の正当な使用者のパスワードで暗号化された暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書、並びに該パスワードをチェックするためのパスワードチェック用データが格納され、上記暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書にアクセスする際には、使用者が入力したパスワードを上記パスワードチェック用データを用いてチェックし、正当な使用者であると確認された場合のみアクセスを許可する請求項20に記載の電子認証公証システム。

【請求項23】前記着脱可能な記憶媒体が、内蔵時計、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するデジタル署名生成プログラム、並びにそれらのプ

ログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたICカードであり、

前記サービス提供者および各サービス享受者は、該ICカードを用いて、秘密鍵と公開鍵の生成および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ICカードに格納し、署名生成時には署名対象のデータに上記内蔵時計の日時データを付加したデータを秘密鍵で暗号化して署名生成する請求項20に記載の電子認証公証システム。

10 【請求項24】前記ICカードは、署名生成の直前に、時刻管理機関が送信する正確な時刻を示す標準時刻データを受信し、該標準時刻データに基づいて内蔵時計を調整する請求項23に記載の電子認証公証システム。

【請求項25】前記ICカードは無線受信装置を備え、該無線受信装置により受信した前記時刻管理機関からの標準時刻データに基づいて内蔵時計を調整する請求項24に記載の電子認証公証システム。

【請求項26】前記着脱可能な記憶媒体内の秘密鍵、公開鍵、および証明書をを用いて署名を行なったとき署名履歴を該記憶媒体内に記憶しておくとともに、該記憶媒体内の秘密鍵、公開鍵、および証明書が新たなデータに変更されたとき、署名履歴を参照して必要があれば、以前に使用した秘密鍵、公開鍵、および証明書を別領域に記憶しておく請求項20に記載の電子認証公証システム。

【請求項27】会員認証局の端末と、個人認証局の端末と、申込者の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、

30 あらかじめ、各申込者に対し、その申込者の公開鍵とその公開鍵がその申込者のものであることを証明する証明書とを含むデジタルデータである個人認証書が前記個人認証局から配布されており、

前記申込者の端末から前記会員認証局の端末に、個人認証書を添付した会員登録申込書を送信し、

前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信し、

前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、前記会員認証局の端末で、その確認結果に基づいて前記申込者の会員資格の審査を行ない、

40 審査の結果、会員資格有りの場合は、前記会員認証局から前記申込者に暗号鍵生成プログラムを内蔵したICカードを配布し、

該ICカード中で、申込者の公開鍵と秘密鍵を生成するとともに、生成した公開鍵を含む申込者に関する所定の情報を所定のフォーマットでまとめたデータである会員証を作成し、

前記申込者の端末から前記会員認証局の端末に、前記会員証を送信し、

50 前記会員認証局の端末で、前記申込者の公開鍵を含む会員証が確かにその者のものであることを証明する証明書

を作成して、申込者の端末に送信し、前記申込者の端末で、受信した証明書の前記ICカードに格納することを特徴とする電子認証システム。

【請求項28】会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の抹消の申込みを送信し、

前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信し、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、本人からの登録抹消依頼であることを確認した上で、会員登録の抹消を行なうことを特徴とする電子認証システム。

【請求項29】会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の有効性の確認依頼を送信し、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信し、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、前記個人認証書と会員証で特定される会員の会員登録の有効性を確認し、その確認結果を前記会員の端末に送信することを特徴とする電子認証システム。

【請求項30】団体の構成員の端末が該団体内ネットワークを介して相互に接続され、該団体の構成員である登録責任者の端末が認証機関の端末とネットワークを介して相互に接続されているシステムにおいて、該団体の構成員の公開鍵の認証機関への登録および認証機関から証明書を発行してもらう処理を、該団体の登録責任者が代行して行なう電子認証システムであって、公開鍵の登録を申請する構成員の端末において、その構成員が登録しようとしている公開鍵を認証機関の公開鍵で暗号化して、前記登録責任者の端末に送信し、前記登録責任者の端末において、受信した構成員の暗号化公開鍵に登録責任者のデジタル署名を付して、前記認証機関の端末に送信し、前記認証機関の端末において、前記登録責任者の端末から送信されたデジタル署名付きの暗号化公開鍵を受信し、前記登録責任者のデジタル署名を確認した後、前

記認証機関の秘密鍵で該暗号化公開鍵を復号し、復号した公開鍵の証明書を作成し、該証明書を前記団体の公開鍵および／または前記構成員の公開鍵で暗号化して、前記登録責任者の端末または前記構成員の端末に送信することを特徴とする電子認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子認証公証方法およびそのシステムに関する。

【0002】

【従来の技術】近年、インターネットのようなオープンなネットワーク環境において、暗号技術を用いた安全な電子商取引が行われるようになってきた。

【0003】一般に、情報の暗号化に際しては、暗号アルゴリズムと暗号鍵とが必要である。暗号アルゴリズムとは、平文と呼ばれる誰でも正しい内容を理解できる情報を、暗号文と呼ばれる全く意味の分からない形の情報に変換する処理手順（暗号化）、およびその逆変換を行う処理手順（復号化）のことである。暗号鍵とは、上記暗号アルゴリズムの変換処理で使用する制御パラメータである。同じ暗号アルゴリズムを使って平文を暗号化しても、その際に使用する暗号鍵が異なると異なる暗号文に変換される。そのため、ある暗号文をもとの平文に正しく復号化するためには、暗号化時に使用したのと同じ暗号鍵、あるいは暗号化時に使用した暗号鍵と対になった暗号鍵が必要となる。前者のように、暗号化時と復号化時に全く同じ暗号鍵を使用する暗号アルゴリズムを対称鍵暗号、あるいは共通鍵暗号といい、後者のように、暗号化時と復号化時に異なる暗号鍵を使用する暗号アルゴリズムを非対称鍵暗号、あるいは公開鍵暗号という。

【0004】共通鍵暗号は、処理速度が高速であるが、鍵の管理に手間がかかる。一方、公開鍵暗号は、処理速度は遅いが、鍵の管理が容易であり、またデジタル署名にも利用できる。

【0005】すなわち、公開鍵暗号では、暗号化および復号化に使用する二つの暗号鍵の非対称性により、一方の鍵（公開鍵）を公に（すべての人に開示）することが可能である。そのため、共通鍵暗号に比べて暗号鍵の管理が比較的容易であり、かつ、認証のためのデジタル署名に利用可能であるといった利点もある。しかし、公開鍵暗号の運用に際しては、それら公にされた公開鍵とその所有者との対応関係が保証されなければならない。なぜなら、もし不正者AがユーザBになりすましてBの公開鍵を公にした場合（その公開鍵に対応した秘密鍵はAが所有している）、ユーザCは、電子署名を確認することにより不正者AをユーザBだと認証してしまうからである。さらに、その結果として、ユーザBに宛てた情報がすべて不正者Aに漏れてしまうことになる。したがって、公開鍵暗号利用環境を構築する際には、公開鍵と

その所有者との対応関係を保証する手段が必要となる。

【0006】認証局 (Certification Authority) は、インターネットのように大規模でオープンなネットワークにおいて、このような課題を解決する手段の一つであり、CCITT (The International Telegraph and Telephone Consultative Committee) の勧告X.509で認証局と証明書を用いた認証の枠組みが規定されている。証明書とは、その証明書の所有者の公開鍵であり、他のいくつかの情報とともに、それを発行した認証局の秘密鍵を用いた暗号化、すなわちデジタル署名により、偽造不可能な形にしたデータのことである。システムを利用するすべてのエンティティは、認証局の証明書 (公開鍵) だけを安全に保持し、他のエンティティの証明書に付けられた認証局のデジタル署名を確認することで、その証明書に含まれた公開鍵の正当性の確認および認証を行なうことが可能となる。

【0007】

【発明が解決しようとする課題】ところで、インターネットのようなネットワーク環境における電子商取引は、消費者-販売店 (モール) 間での電子商取引から、企業-企業間の電子商取引へと拡大していく兆しがある。企業間電子商取引では、個々の取引を安全に行なうだけでなく、取引内容やそのような取引が行なわれたという事実を保証し、その証拠をある一定の期間保管しておく “公証サービス” の重要性が高まっていくものと考えられる。また、そのような公証サービスは、消費者電子商取引への適用や、電子商取引以外への適用 (遺言等、現在公証人役場で公証人が提供しているサービス) も考えられる。

【0008】しかしながら、ISOでは、“否認防止 (Non Repudiation)” 技術の標準化は進められているが、フレームワーク的なものであり、実現方式を細かく規定したものとはなっていない。また、オンラインで受け取った電子情報を保管するサービスはあるが (電子貸し金庫)、取引という観点がないため、上記 “公証サービス” は実現できない。さらに、法務省民事部が電子取引における電子認証・公証制度の必要性を提言しているが、これも実現方式を細かく規定したものではない。

【0009】本発明は、オープンなネットワーク環境において電子商取引を行なう際に必要とされる認証・公証サービス (電子情報署名・保管サービス) を実現することを目的とする。

【0010】

【課題を解決するための手段】上記目的を達成するため、請求項1に係る発明は、公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを受信する複数のサービス享受者がそれぞれ使用する複数のサービス享受装置とが、ネットワークを介して相互に接続されているシステムに適用する電子認証公証方法であって、前記サービス提供装置から、契約内容を

含む契約情報を、契約者である各サービス享受者のサービス享受装置に、それぞれ送信するステップと、該契約情報を受信した各サービス享受装置で、該契約情報にサービス享受者の署名を付けた一者署名付き契約情報を作成し、前記サービス提供装置に送信するステップと、前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報をまとめて一つの文書にするとともに、該文書にサービス提供者の署名を付けたサービス提供者署名付き契約情報を作成するステップと、前記サービス提供装置で、作成したサービス提供者署名付き契約情報を保管するステップと、前記サービス提供者署名付き契約情報を、前記サービス提供装置から前記各サービス享受装置に送信するステップとを備えたことを特徴とする。

【0011】請求項2に係る発明は、公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを受信する複数のサービス享受者が使用する複数のサービス享受装置と、前記サービス提供者および各サービス享受者の公開鍵が確かにその者の公開鍵であることを保証する証明書を発行する認証機関の端末装置とが、ネットワークを介して相互に接続されているシステムに適用する電子認証公証方法であって、前記サービス提供装置で、前記サービス提供者の公開鍵と秘密鍵とを生成するステップと、前記各サービス享受装置で、それぞれ、前記各サービス享受者の公開鍵と秘密鍵とを生成するステップと、前記サービス提供装置および各サービス享受装置から、生成した公開鍵を前記認証機関の端末装置に送信するステップと、前記認証機関の端末装置で、受信した公開鍵ごとに、その公開鍵に対応する証明書を作成し、それぞれ対応する前記サービス提供装置および各サービス享受装置に送信するステップと、前記サービス提供装置および各サービス享受装置で、前記証明書をそれぞれ受信するステップと、前記各サービス享受装置から、それぞれ、契約内容その他の契約に係る各種の情報を前記サービス提供装置に送信するステップと、前記サービス提供装置において、前記各サービス享受装置からそれぞれ送られてくる契約に係る各種の情報をまとめて契約内容を含む契約情報を作成し、前記各サービス享受装置にそれぞれ送信するステップと、前記各サービス享受装置で、それぞれ、受信した契約情報にサービス享受者の証明書を含む付属情報を所定の順序で連結したデータを作成し、該連結したデータを所定の一方方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス享受者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせて一者署名付き契約情報を作成し、該一者署名付き契約情報を前記サービス提供装置に送信するステップと、前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契

約情報から契約情報並びに各サービス享受者が付加した付属情報および署名を取り出し、取り出した情報とサービス提供者の証明書を含む付属情報とを所定の順序で連結したデータを作成し、該連結したデータを所定の一方方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス提供者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせてサービス提供者署名付き契約情報を作成するステップと、前記サービス提供装置で、作成したサービス提供者署名付き契約情報を保管するステップと、前記サービス提供者署名付き契約情報を、前記サービス提供装置から前記各サービス享受装置に送信するステップとを備えたことを特徴とする。

【0012】請求項3に係る発明は、請求項2において、前記ネットワークを介したサービス提供者およびサービス享受者と認証機関との間の通信を、認証機関の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なうこととしたものである。

【0013】請求項4に係る発明は、請求項1または2において、前記ネットワークを介したサービス提供者とサービス享受者との間の通信を、互いの証明書を交換し、サービス提供者の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なうこととしたものである。

【0014】請求項5に係る発明は、請求項1または2において、前記サービス提供者および各サービス享受者には、前記認証機関の公開鍵である認証機関証明書が格納されている、前記サービス提供装置およびサービス享受装置に着脱可能な、記憶媒体が、あらかじめ配布されており、前記サービス提供者および各サービス享受者の公開鍵および秘密鍵、並びに、前記認証機関が発行した証明書は、該記憶媒体に格納されることとしたものである。

【0015】請求項6に係る発明は、請求項5において、前記着脱可能な記憶媒体が、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するデジタル署名生成プログラム、並びにそれらのプログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたICカードであり、前記サービス提供者および各サービス享受者は、該ICカードを用いて、秘密鍵と公開鍵の生成、および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ICカードに格納することとしたものである。

【0016】請求項7に係る発明は、請求項5において、前記着脱可能な記憶媒体には、当該記憶媒体の正当な使用者のパスワードで暗号化された暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書、並びに該パスワードをチェックするためのパスワードチェック用データが格納され、上記暗号化秘密鍵、暗号化公開鍵、および暗

号化自証明書にアクセスする際には、使用者が入力したパスワードを上記パスワードチェック用データを用いてチェックし、正当な使用者であると確認された場合のみアクセスを許可することとしたものである。

【0017】請求項8に係る発明は、請求項5において、前記着脱可能な記憶媒体が、内蔵時計、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するデジタル署名生成プログラム、並びにそれらのプログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたICカードであり、前記サービス提供者および各サービス享受者は、該ICカードを用いて、秘密鍵と公開鍵の生成および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ICカードに格納し、署名生成時には署名対象のデータに上記内蔵時計の日時データを付加したデータを秘密鍵で暗号化して署名生成することとしたものである。

【0018】請求項9に係る発明は、請求項8において、前記ICカードが、署名生成の直前に、時刻管理機関が送信する正確な時刻を示す標準時刻データを受信し、該標準時刻データに基づいて内蔵時計を調整することとしたものである。

【0019】請求項10に係る発明は、請求項9において、前記ICカードは無線受信装置を備え、該無線受信装置により受信した前記時刻管理機関からの標準時刻データに基づいて内蔵時計を調整することとしたものである。

【0020】請求項11に係る発明は、請求項5において、前記着脱可能な記憶媒体内の秘密鍵、公開鍵、および証明書をを用いて署名を行なったとき署名履歴を該記憶媒体内に記憶しておくとともに、該記憶媒体内の秘密鍵、公開鍵、および証明書が新たなデータに変更されたとき、署名履歴を参照して必要があれば、以前に使用した秘密鍵、公開鍵、および証明書を別領域に記憶しておくこととしたものである。

【0021】請求項12に係る発明は、会員認証局の端末と、個人認証局の端末と、申込者の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、あらかじめ、各申込者が、その申込者の公開鍵とその公開鍵がその申込者のものであることを証明する証明書とを含むデジタルデータである個人認証書の配布を前記個人認証局から受けるステップと、前記申込者の端末から前記会員認証局の端末に、個人認証書を添付した会員登録申込書を送信するステップと、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、前記会員認証局の端末で、そ

の確認結果に基づいて前記申込者の会員資格の審査を行なうステップと、審査の結果、会員資格有りの場合は、前記会員認証局から前記申込者に暗号鍵生成プログラムを内蔵したICカードを配布するステップと、該ICカード中で、申込者の公開鍵と秘密鍵を生成するとともに、生成した公開鍵を含む申込者に関する所定の情報を所定のフォーマットでまとめたデータである会員証を作成するステップと、前記申込者の端末から前記会員認証局の端末に、前記会員証を送信するステップと、前記会員認証局の端末で、前記申込者の公開鍵を含む会員証が確かにその者のものであることを証明する証明書を作成して、申込者の端末に送信するステップと、前記申込者の端末で、受信した証明書を前記ICカードに格納するステップとを備えたことを特徴とする。

【0022】請求項13に係る発明は、会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の抹消の申込みを送信するステップと、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、本人からの登録抹消依頼であることを確認した上で、会員登録の抹消を行なうステップとを備えたことを特徴とする。

【0023】請求項14に係る発明は、会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の有効性の確認依頼を送信するステップと、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、前記個人認証書と会員証で特定される会員の会員登録の有効性を確認し、その確認結果を前記会員の端末に送信するステップとを備えたことを特徴とする。

【0024】請求項15に係る発明は、団体の構成員の端末が該団体内ネットワークを介して相互に接続され、該団体の構成員である登録責任者の端末が認証機関の端末とネットワークを介して相互に接続されているシステムにおいて、該団体の構成員の公開鍵の認証機関への登

録および認証機関から証明書を発行してもらう処理を、該団体の登録責任者が代行して行なう電子認証方法であって、公開鍵の登録を申請する構成員の端末において、その構成員が登録しようとしている公開鍵を認証機関の公開鍵で暗号化して、前記登録責任者の端末に送信するステップと、前記登録責任者の端末において、受信した構成員の暗号化公開鍵に登録責任者のデジタル署名を付して、前記認証機関の端末に送信するステップと、前記認証機関の端末において、前記登録責任者の端末から送信されたデジタル署名付きの暗号化公開鍵を受信し、前記登録責任者のデジタル署名を確認した後、前記認証機関の秘密鍵で該暗号化公開鍵を復号し、復号した公開鍵の証明書を作成し、該証明書を前記団体の公開鍵および／または前記構成員の公開鍵で暗号化して、前記登録責任者の端末または前記構成員の端末に送信するステップとを備えたことを特徴とする。

【0025】請求項16に係る発明は、公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者がそれぞれ使用する複数のサービス享受装置とが、ネットワークを介して相互に接続されて構成される電子認証公証システムであって、前記サービス提供装置から、契約内容を含む契約情報を、契約者である各サービス享受者のサービス享受装置に、それぞれ送信し、該契約情報を受信した各サービス享受装置で、該契約情報にサービス享受者の署名を付けた一者署名付き契約情報を作成して、前記サービス提供装置に送信し、前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報をまとめて一つの文書にするとともに、該文書にサービス提供者の署名を付けたサービス提供者署名付き契約情報を作成し、該作成したサービス提供者署名付き契約情報を保管するとともに、前記各サービス享受装置に送信することを特徴とする。

【0026】請求項17に係る発明は、公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者が使用する複数のサービス享受装置と、前記サービス提供者および各サービス享受者の公開鍵が確かにその者の公開鍵であることを保証する証明書を発行する認証機関の端末装置とが、ネットワークを介して相互に接続されて構成される電子認証公証システムであって、前記サービス提供装置で、前記サービス提供者の公開鍵と秘密鍵とを生成し、前記各サービス享受装置で、それぞれ、前記各サービス享受者の公開鍵と秘密鍵とを生成し、前記サービス提供装置および各サービス享受装置から、生成した公開鍵を前記認証機関の端末装置に送信し、前記認証機関の端末装置で、受信した公開鍵ごとに、その公開鍵に対応する証明書を作成し、それぞれ対応する前記サービス提供装置および各サービス享受装置に送信し、前記サ

ービス提供装置および各サービス享受装置で、前記証明書
書をそれぞれ受信し、前記各サービス享受装置から、そ
れぞれ、契約内容その他の契約に係る各種の情報を前記
サービス提供装置に送信し、前記サービス提供装置にお
いて、前記各サービス享受装置からそれぞれ送られてく
る契約に係る各種の情報をまとめて契約内容を含む契約
情報を作成し、前記各サービス享受装置にそれぞれ送信
し、前記各サービス享受装置で、それぞれ、受信した契
約情報にサービス享受者の証明書を含む付属情報を所定
の順序で連結したデータを作成し、該連結したデータを
所定の一方方向性関数で圧縮した圧縮子を生成し、該圧縮
子をサービス享受者の秘密鍵で暗号化した署名を生成
し、前記連結したデータに該署名を合わせて一者署名付
き契約情報を作成し、該一者署名付き契約情報を前記サ
ービス提供装置に送信し、前記サービス提供装置で、前
記各サービス享受装置からそれぞれ送信された一者署名
付き契約情報を受信し、受信した複数の一者署名付き契
約情報から契約情報並びに各サービス享受者が付加した
付属情報および署名を取り出し、取り出した情報とサー
ビス提供者の証明書を含む付属情報とを所定の順序で連
結したデータを作成し、該連結したデータを所定の一方
方向性関数で圧縮した圧縮子を生成し、該圧縮子をサー
ビス提供者の秘密鍵で暗号化した署名を生成し、前記連結
したデータに該署名を合わせてサービス提供者署名付き
契約情報を作成し、前記サービス提供装置で、作成した
サービス提供者署名付き契約情報を保管し、前記サービ
ス提供者署名付き契約情報を、前記サービス提供装置か
ら前記各サービス享受装置に送信することを特徴とす
る。

【0027】請求項18に係る発明は、請求項17にお
いて、前記ネットワークを介したサービス提供者および
サービス享受者と認証機関との間の通信を、認証機関の
公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その
交換した鍵と共通鍵暗号とを使用した暗号通信により行
なうこととしたものである。

【0028】請求項19に係る発明は、請求項16また
は17において、前記ネットワークを介したサービス提
供者とサービス享受者との間の通信を、互いの証明書を
交換し、サービス提供者の公開鍵と公開鍵暗号とを使用
して鍵交換を行ない、その交換した鍵と共通鍵暗号とを
使用した暗号通信により行なうこととしたものである。

【0029】請求項20に係る発明は、請求項16また
は17において、前記サービス提供者および各サービス
享受者には、前記認証機関の公開鍵である認証機関証明
書が格納されている、前記サービス提供装置およびサー
ビス享受装置に着脱可能な、記憶媒体が、あらかじめ配
布されており、前記サービス提供者および各サービス享
受者の公開鍵および秘密鍵、並びに、前記認証機関が発
行した証明書は、該記憶媒体に格納されることとしたも
のである。

【0030】請求項21に係る発明は、請求項20にお
いて、前記着脱可能な記憶媒体が、秘密鍵と公開鍵を生
成する暗号鍵生成プログラムおよび入力したデータを秘
密鍵で暗号化して署名を生成し出力するデジタル署名
生成プログラム、並びにそれらのプログラムを実行して
暗号鍵生成や署名生成を実行する処理装置を備えたIC
カードであり、前記サービス提供者および各サービス享
受者は、該ICカードを用いて、秘密鍵と公開鍵の生
成、および署名の生成を行なうとともに、生成した秘密
鍵と公開鍵および前記認証機関から送付された証明書は
該ICカードに格納することとしたものである。

【0031】請求項22に係る発明は、請求項20にお
いて、前記着脱可能な記憶媒体には、当該記憶媒体の正
当な使用者のパスワードで暗号化された暗号化秘密鍵、
暗号化公開鍵、および暗号化自証明書、並びに該パス
ワードをチェックするためのパスワードチェック用データ
が格納され、上記暗号化秘密鍵、暗号化公開鍵、および
暗号化自証明書にアクセスする際には、使用者が入力し
たパスワードを上記パスワードチェック用データを用い
てチェックし、正当な使用者であると確認された場合の
みアクセスを許可することとしたものである。

【0032】請求項23に係る発明は、請求項20にお
いて、前記着脱可能な記憶媒体が、内蔵時計、秘密鍵と
公開鍵を生成する暗号鍵生成プログラムおよび入力した
データを秘密鍵で暗号化して署名を生成し出力するディ
ジタル署名生成プログラム、並びにそれらのプログラム
を実行して暗号鍵生成や署名生成を実行する処理装置を
備えたICカードであり、前記サービス提供者および各
サービス享受者は、該ICカードを用いて、秘密鍵と公
開鍵の生成および署名の生成を行なうとともに、生成し
た秘密鍵と公開鍵および前記認証機関から送付された証
明書は該ICカードに格納し、署名生成時には署名対象
のデータに上記内蔵時計の日時データを付加したデータ
を秘密鍵で暗号化して署名生成することとしたものであ
る。

【0033】請求項24に係る発明は、請求項23にお
いて、前記ICカードが、署名生成の直前に、時刻管理
機関が送信する正確な時刻を示す標準時刻データを受信
し、該標準時刻データに基づいて内蔵時計を調整するこ
ととしたものである。

【0034】請求項25に係る発明は、請求項24にお
いて、前記ICカードは無線受信装置を備え、該無線受
信装置により受信した前記時刻管理機関からの標準時刻
データに基づいて内蔵時計を調整することとしたもので
ある。

【0035】請求項26に係る発明は、請求項20にお
いて、前記着脱可能な記憶媒体内の秘密鍵、公開鍵、お
よび証明書をを用いて署名を行なったとき署名履歴を該記
憶媒体内に記憶しておくとともに、該記憶媒体内の秘密
鍵、公開鍵、および証明書が新たなデータに変更された

とき、署名履歴を参照して必要があれば、以前に使用した秘密鍵、公開鍵、および証明書を別領域に記憶しておくこととしたものである。

【0036】請求項27に係る発明は、会員認証局の端末と、個人認証局の端末と、申込者の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、あらかじめ、各申込者に対し、その申込者の公開鍵とその公開鍵がその申込者のものであることを証明する証明書とを含むデジタルデータである個人認証書が前記個人認証局から配布されており、前記申込者の端末から前記会員認証局の端末に、個人認証書を添付した会員登録申込書を送信し、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信し、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、前記会員認証局の端末で、その確認結果に基づいて前記申込者の会員資格の審査を行ない、審査の結果、会員資格有りの場合は、前記会員認証局から前記申込者に暗号鍵生成プログラムを内蔵したICカードを配布し、該ICカード中で、申込者の公開鍵と秘密鍵を生成するとともに、生成した公開鍵を含む申込者に関する所定の情報を所定のフォーマットでまとめたデータである会員証を作成し、前記申込者の端末から前記会員認証局の端末に、前記会員証を送信し、前記会員認証局の端末で、前記申込者の公開鍵を含む会員証が確かにその者のものであることを証明する証明書を作成して、申込者の端末に送信し、前記申込者の端末で、受信した証明書を前記ICカードに格納することを特徴とする。

【0037】請求項28に係る発明は、会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の抹消の申込みを送信し、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信し、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、本人からの登録抹消依頼であることを確認した上で、会員登録の抹消を行なうことを特徴とする。

【0038】請求項29に係る発明は、会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の有効性の確認依頼を送信し、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確

認依頼を送信し、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、前記個人認証書と会員証で特定される会員の会員登録の有効性を確認し、その確認結果を前記会員の端末に送信することを特徴とする。

【0039】請求項30に係る発明は、団体の構成員の端末が該団体内ネットワークを介して相互に接続され、該団体の構成員である登録責任者の端末が認証機関の端末とネットワークを介して相互に接続されているシステムにおいて、該団体の構成員の公開鍵の認証機関への登録および認証機関から証明書を発行してもらう処理を、該団体の登録責任者が代行して行なう電子認証システムであって、公開鍵の登録を申請する構成員の端末において、その構成員が登録しようとしている公開鍵を認証機関の公開鍵で暗号化して、前記登録責任者の端末に送信し、前記登録責任者の端末において、受信した構成員の暗号化公開鍵に登録責任者のデジタル署名を付して、前記認証機関の端末に送信し、前記認証機関の端末において、前記登録責任者の端末から送信されたデジタル署名付きの暗号化公開鍵を受信し、前記登録責任者のデジタル署名を確認した後、前記認証機関の秘密鍵で該暗号化公開鍵を復号し、復号した公開鍵の証明書を作成し、該証明書を前記団体の公開鍵および／または前記構成員の公開鍵で暗号化して、前記登録責任者の端末または前記構成員の端末に送信することを特徴とする。

【0040】

【発明の実施の形態】以下、図面を用いて、本発明の実施の形態を説明する。

【0041】図1は、本発明の第1の実施の形態に係る電子公証システムのシステム図である。同図において、100は公証サービスを提供するサービス提供者、130はサービス提供者が使用するサービス提供装置、110と111は公証サービスを受受するサービス享受者、140と141はサービス享受者110と111がそれぞれ使用するサービス享受装置を示す。100、110、111は擬人化して図示してあるが、自然人とは限らず、法人などの団体であってもよい。170は各者が本人であることを保証する証明書を発行する認証機関、180は本システムで用いるICカード120を発行するICカード発行機関である。

【0042】サービス提供装置130およびサービス享受装置140、141は、通信網180に接続されており相互に各種情報の授受が可能である。また、図示していないが、認証機関170内に設けられた証明書発行業務を行なう端末装置が、上記通信網180に接続されており、サービス提供装置130およびサービス享受装置140、141と各種情報の授受が可能である。

【0043】図1を参照して、本システムにおける公証サービスの流れを説明する。サービス享受者110と111との間には、あらかじめ何らかの契約を行なう合意が取れているものとする。サービスの前準備として、サービス享受者110、111とサービス提供者100は、それぞれ、認証機関170に対してICカード120の発行を申し込む。認証機関170は、ICカード発行の申込みを受け付け、種々の方法でその申込者が本人であることを確認し、ICカード120を発行する。ここでは、サービス提供者100に対してICカード121を、サービス享受者110に対してICカード122を、サービス享受者111に対してICカード123を、それぞれ発行したとする。なお、図1において、点線の矢印はオフラインで各者間のやり取りを行なうことを示し、実線の矢印は通信網180を介したオンラインでのやり取りを行なうことを示す。

【0044】認証機関170はICカード120をどのような方法で用意してもよいが、本システムで用いるICカード(図2で後述)は規格化されたものである。ICカード発行機関180が作成したICカード120を用いることとしている。

【0045】サービス提供者100とサービス享受者110、111は、それぞれ、ICカード121~123内に自分の公開鍵と秘密鍵を生成する作業を行う。ICカードは、公開鍵と秘密鍵を生成する機能を備えている。次に各者100、110、111は、それぞれ、生成した自分の公開鍵150、151、152を認証機関170に送り、証明書153、154、155を取得する。公開鍵150~152を送信して証明書153~155を取得する処理はオンラインで行なう。受信した証明書153~155は、それぞれ、各者100、110、111のICカード121~123に格納される。

【0046】以上で、公証サービスを行なうための前準備を終える。

【0047】公証サービスは以下のような手順で行なわれる。まず、所定の契約内容で契約することに合意しているサービス享受者110と111は、それぞれ、契約内容をサービス提供者100にオンラインで(オフラインでもよい)送付する。サービス提供者100は、その契約内容を総合して一定の書式にまとめた契約情報160を作成し、サービス享受者110、111にそれぞれオンラインで(オフラインでもよい)送付する。サービス享受者110、111は、それぞれ、その契約情報160の内容を確認し、依存がなければ、自分のICカード122、123をサービス享受装置140、141に挿入して、契約情報160にデジタル署名を付ける。ICカードは、署名生成機能を備えている。ここまでで、サービス享受者110側では一者署名付き契約情報161が作成され、サービス享受者111側では一者署名付き契約情報162が作成されたことになる。

【0048】これらの一者署名付き契約情報161、162は、サービス享受装置140、141から、それぞれサービス提供装置130に返送される。サービス提供者100は、サービス享受者110の署名が付いた一者署名付き契約情報161とサービス享受者111の署名が付いた一者署名付き契約情報162とを合わせて1つの文書にするとともに、該文書にICカード121を用いてデジタル署名を付して、三者署名付き契約情報163を作成する。サービス提供者100は、この三者署名付き契約情報163をサービス享受者110、111にそれぞれ送付するとともに、一定期間これを保管する。

【0049】以上により、サービス提供者100による公証サービス(サービス享受者110、111間の契約に係る公証)が行なわれた。サービス提供者100は、三者署名付き契約情報163を一定期間保管している。この三者署名付き契約情報163がある限り、その契約内容および契約が行なわれた事実を保証できる。

【0050】なお、図1ではサービス享受者が二者の場合を示したが、サービス享受者が三者以上いる場合も同様である。例えば、サービス享受者が三者いる場合は、サービス提供者はその三者から送られてくる一者署名付き契約情報を一文書にして自分の署名を付け、四者署名付き契約情報(サービス提供者署名付き契約情報)を作成して保管することになる。

【0051】また、本実施の形態のシステムにおいて、サービス提供装置130やサービス享受装置140、141と認証機関170の端末装置とのオンラインでのデータのやり取り(証明書発行時)は、暗号通信で行なうものとする。すなわち、まず認証機関170の公開鍵(後述する認証機関証明書513)と公開鍵暗号とを使って鍵交換を行ない、その交換した鍵と共通鍵暗号とにより暗号通信を行なう。また、サービス提供装置130とサービス享受装置140、141とのオンラインでのデータのやり取り(公証サービス時)も、同様に暗号通信で行なうものとする。すなわち、まず、互いの証明書を交換し、次にサービス提供者100の公開鍵と公開鍵暗号とを使って鍵交換を行ない、その交換した鍵と共通鍵暗号とにより暗号通信を行なう。上記暗号通信において、交換した鍵は一連のサービス終了まで使用する。

【0052】図2は、図1のICカード発行機関180が発行するICカード120の内部構成図である。認証機関170がサービス提供者100、およびサービス享受者110、111に配布するICカード121~123はこの構成のものである。同図に示すように、ICカード120は、リーダライタインタフェース201と、CPU(中央処理装置)202と、メモリ203とを有している。これら各部はバス200によって相互に接続されている。

【0053】CPU202は、演算機能を備え、ICカ

ード120内の処理の全体を制御する。リーダライタインタフェース201は、後述する各者の装置のリーダライタ320、420との間でデータのやり取りを行なうためのインタフェースである。メモリ203には、端末・ICカード間データ送受信プログラムが記憶されている領域203a、ICカード制御プログラムが記憶されている領域203b、暗号鍵生成プログラムが記憶されている領域203c、署名生成プログラムが記憶されている領域203d、およびデータ記憶領域203eが設けられている。メモリ203はこのICカード120をリーダライタから引き抜いた状態でも記憶内容を保持する不揮発なメモリであり、CPU202から見ると、プログラムを記憶した領域203a~203dは読み出しのみ可能な領域、データ記憶領域203eは読み出し・書き込みが可能な領域である。

【0054】メモリ203に記憶されている端末・ICカード間データ送受信プログラムは、リーダライタを介して当該ICカードと端末との間でデータのやり取りを行なう際に使用するプログラムである。ICカード制御プログラムは、このICカード全体の動作を制御（データの流れの制御やアクセスコントロールなど）するプログラムである。暗号鍵生成プログラムは、秘密鍵と公開鍵を生成するプログラムである。署名生成プログラムは、外から与えられたデータに対してデジタル署名を付けて返す処理を行なうプログラムである。データ記憶領域203eに記憶するデータについては、図5で詳しく説明する。

【0055】図3は、サービス提供装置130の内部構成図である。同図に示すように、サービス提供装置130は、端末300、リーダライタ320、および外部記憶装置340を備えている。

【0056】端末300は、リーダライタインタフェース311、外部記憶装置インタフェース312、通信網インタフェース313、CPU314、入出力装置315、およびメモリ316を備えている。これら各部は、バス310によって相互に接続されている。リーダライタインタフェース311は、リーダライタ320との間でデータのやり取りを行なうためのインタフェースである。外部記憶装置インタフェース312は、外部記憶装置340との間でデータのやり取りを行なうためのインタフェースである。通信網インタフェース313は、通信網180を介して別の端末との間でデータのやり取りを行なう際のインタフェースである。CPU314は、演算機能を備え、このサービス提供装置130全体の動作を制御する。入出力装置315は、各種の情報を表示するディスプレイや、ユーザがコマンドやデータを入力するためのキーボードやマウスなどからなる。

【0057】メモリ316には、端末・ICカード間データ送受信プログラムが記憶されている領域316a、サービス提供プログラムが記憶されている領域316

b、通信プログラムが記憶されている領域316c、暗号プログラムが記憶されている領域316d、およびデータ記憶領域316eが設けられている。メモリ316は電源を落とすと内容が失われる揮発性のメモリでよい。メモリ316内のプログラムやデータは、必要に応じてハードディスクなどの外部記憶装置340から読み込まれ、保存が必要なデータは外部記憶装置340に書き込まれる。

【0058】メモリ316に格納されている端末・ICカード間データ送受信プログラムは、リーダライタ320を介して当該端末300とICカードとの間でデータのやり取りを行なうプログラムである。サービス提供プログラムは、図1で説明した公証サービス（前準備の処理も含む）を提供する際の動作全体を制御するプログラムである。通信プログラムは、通信網180を介して本端末300と他の端末との通信を行なうプログラムである。暗号プログラムは、通信網180を介して他の端末と各種情報をやり取りする際に暗号通信を行なうプログラムである。

【0059】リーダライタ320は、CPU331、リーダライタ制御プログラム領域332、端末インタフェース333、およびICカードインタフェース334を備えている。これら各部は、バス330によって相互に接続されている。CPU331は、このリーダライタ320の動作（リーダライタ320に挿入されたICカード120と端末300との間のデータのやり取りに係る各種の動作）の制御を行なうCPUである。CPU331が実行するリーダライタ制御プログラムは、リーダライタ制御プログラム領域332に格納されている。端末インタフェース333は、端末300との間でデータのやり取りを行なうためのインタフェースである。ICカードインタフェース334は、このリーダライタ320に挿入されたICカードとの間でデータのやり取りを行なうためのインタフェースである。

【0060】図4は、サービス享受装置140の内部構成図である。サービス享受装置140も同じ構成である。サービス享受装置140は、図3で説明したサービス提供装置130とほぼ同じ構成であるので、説明は省略する。図3の各部に付された300番台の番号を400番台に読み替えばよい。ただし、図3のサービス提供装置130は公証サービスを提供する側の装置であるので領域316bにはサービス提供プログラムが格納されているが、図4のサービス享受装置140は公証サービスを享受する側の装置であるので領域416bにはサービス享受プログラムが格納されている。サービス享受プログラムは、図1で説明した公証サービス（前準備の処理も含む）を享受する際の動作全体を制御するプログラムである。

【0061】図5は、図2で説明したICカード120のデータ記憶領域203eの内容を示すブロック図であ

る。データ記憶領域203eは、外部出力禁止領域500と、外部出力許可領域510と、ワーク領域520とからなる。外部出力禁止領域500に格納されているデータは、ICカード120の内部だけで使用するデータであり、ICカード120の外部への出力は禁止される。外部出力許可領域510に格納されているデータは、ICカード120の外部へ出力することができる。ワーク領域520は、ICカード120のCPU202が演算実行の際に使用するワーク領域である。

【0062】外部出力禁止領域500には、秘密鍵501とユーザID502とパスワードチェック用データ503が格納される。秘密鍵501は、このICカード120の正当な使用者が作成して設定する当該使用者の秘密鍵である。ユーザID502は、このICカード120の正当な使用者の識別子である。パスワードチェック用データ503は、ユーザがこのICカードを使用するときに入力するパスワードが正当な使用者のパスワードであるか否かをチェックするために用いるデータである。パスワードチェック用データ503は、パスワードそのものではなく、パスワードを何らかの方向性の関数に通した値とする。

【0063】外部出力許可領域510には、公開鍵511と自証明書512と認証機関証明書513とICカード番号514とが格納される。公開鍵511は、このICカード120の正当な使用者が作成して設定する当該使用者の公開鍵（上記秘密鍵501と対のもの）である。自証明書512は、認証機関170に発行してもらったこのICカード120の正当な使用者（自分）の証明書である。自証明書512には、証明内容と認証機関170の署名とが含まれている。証明内容とは、このICカード120の正当な使用者の公開鍵と他の幾つかの情報からなる。認証機関170の署名は、上記証明内容を一方向関数で圧縮した圧縮子を認証機関170の秘密鍵で暗号化し偽造不可能な形にしたものである。認証機関証明書513は、契約の相手方の証明書により相手方を認証する際に、認証機関170の署名の正当性を確認するための証明書（認証機関170の公開鍵）である。ICカード番号514は、他のICカードと区別するためのICカード固有の番号である。

【0064】上記ICカード120内の各データのうち、認証機関170がICカード120を発行するときに格納済みのデータは、ユーザID502、パスワードチェック用データ503、認証機関証明書513、およびICカード番号514である。なお、ICカード発行時にパスワードチェック用データ503に設定されているデータは、認証機関170が設定した仮パスワードに対応するデータであり、ユーザはカードを受取った後に自分でパスワードを変更する（パスワードチェック用データ503はパスワードの変更に伴って変更される）ことは可能である。

【0065】図6は、図1で説明したシステムにおいて、サービス提供者100が認証機関170よりICカード121を発行してもらう手順を示す流れ図である。同図において、「サービス提供者100」と記載された下側に並べたブロックはサービス提供者100が行なう動作、「認証機関170」と記載された下側に並べたブロックは認証機関170が行なう動作を示す。

【0066】サービス提供者100は、ステップ600でICカード申込書を作成し、ステップ601でICカード申込書を認証機関170に送付する。認証機関170は、ステップ602でそのICカード申込書を受付け、ステップ603でICカード申込書を送付してきた者の身元審査を行なう。身元が確認されたら、ステップ604でユーザ管理情報を更新し、ステップ605でICカード121をサービス提供者100に送付する。サービス提供者100は、ステップ606で、ICカード121を受け取る。

【0067】なお、ユーザ管理情報とは、認証機関170がICカードや証明書を発行したユーザについて管理する各種の情報のことである。また、認証機関170は、図5で説明したICカード121中のデータのうち、ユーザID502にはユーザがICカード申込書に記載したID（認証機関側でIDを付けることにしてもよい）を設定し、パスワードチェック用データ503には仮のパスワードを設定し、認証機関証明書513には当該認証機関170の公開鍵を設定し、ICカード番号514には当該ICカードの番号を設定して、ユーザに送付する。

【0068】図6ではサービス提供者100が認証機関170からICカード121を発行してもらう手順を説明したが、サービス享受者110、111が認証機関170からICカード122、123を発行してもらう手順も同様である。

【0069】図7は、第1の実施の形態において、サービス提供者100が、自ICカード121とサービス提供装置130とを用いて、オンラインで認証機関170より証明書153を発行してもらう手順を示す流れ図である。同図において、「ICカード121」と記載された下側に並べたブロックは、ICカード121内のCPU202がメモリ203内のプログラム（図2）を実行することによる動作であり、特に、全体の流れの制御はICカード制御プログラム（203b）で、サービス提供装置130の端末300との間のデータの送受信は端末・ICカード間データ送受信プログラム（203a）で、秘密鍵と公開鍵の生成は暗号鍵生成プログラム（203c）で、それぞれ、行なう。「サービス提供装置130」と記載された下側に並べたブロックは、サービス提供装置130の端末300内のCPU314がメモリ316内のプログラム（図3）を実行することによる動作であり、特に、全体の流れの制御はサービス提供プロ

グラム(316b)で、ICカード121との間のデータの送受信は端末・ICカード間データ送受信プログラム(316a)で、認証機関170の端末との間でメッセージの送受信(暗号通信)を行なう際の該メッセージの暗号化と復号化は暗号プログラム(316d)で、認証機関170の端末との間のメッセージの送受信は通信プログラム(316c)で、それぞれ、行なう。「認証機関170」と記載された下側に並べたブロックは、認証機関170に備えられた証明書の発行業務を行なう端末における動作を示す。

【0070】サービス提供者100が、サービス提供装置130に接続されているリーダライタ320に自分のICカード121を挿入し、所定の操作を行なうことで図7の手順が開始する。まず、ステップ700で、ICカード121はサービス提供者100からの指示に基づいて秘密鍵および公開鍵を生成し、データ記憶領域203e(図5)内に秘密鍵501および公開鍵511として格納する。次に、ステップ701でICカード番号514と生成した公開鍵511とをサービス提供装置130に送信する。

【0071】サービス提供装置130は、ステップ702で、ICカード番号514と公開鍵511を受信する。次に、ステップ703で証明書要求メッセージ(ICカード番号514、公開鍵511、およびその他の必要な情報を含む)を作成し、ステップ704でその証明書要求メッセージを暗号化し、ステップ705でその暗号化証明書要求メッセージを認証機関170の端末に送信する。なお、上述したようにサービス提供装置130と認証機関170の端末との間では暗号通信を行なうが、そのための共通鍵の交換はステップ705に先立って行なっているものとする。

【0072】認証機関170の端末は、ステップ706で暗号化証明書要求メッセージを受信し、ステップ707で暗号化証明書要求メッセージを復号化する。次に、ステップ708で当該メッセージを送ってきた者の身元確認を行なう。身元が確認されたら、ステップ709で、受信した証明書要求メッセージ中の公開鍵などの情報を認証機関170の秘密鍵で暗号化して証明書を作成する。次に、ステップ710でその証明書を暗号化し、ステップ711でその暗号化証明書をサービス提供装置130に送信する。

【0073】サービス提供装置130は、ステップ712で、暗号化証明書を受信する。ステップ713でその暗号化証明書を復号化し、ステップ714で復号化した証明書をICカード121に送信する。ICカード121は、ステップ715で、証明書を受信し、データ記憶領域203eの自証明書512の領域(図5)に格納する。

【0074】なお、上記図7では、サービス提供者100が証明書を発行してもらう手順を説明したが、サービ

ス享受者110、111が認証機関170から証明書を発行してもらう手順も同様である。図7において、ICカード121をICカード122または123に置き換え、サービス提供装置130をサービス享受装置140または141に置き換えて、同様の手順で行なえばよい。

【0075】図8は、上記図6および図7のICカード発行手順の変形例を示す。図6および図7では、認証機関170からICカードを発行してもらい、ICカードの所有者が自ら鍵生成を行なうとともに、図7の手順でオンラインで証明書を発行してもらうようにしているが、図8のようにして、始めから鍵や証明書が格納されたICカードを発行してもらうようにしてもよい。

【0076】図8の手順では、サービス提供者100は、ステップ800でICカード申込書を作成し、ステップ801でICカード申込書を認証機関170にオフラインで送付する。認証機関170では、ステップ802でICカード申込書を受け、ステップ803で身元審査を行なう。身元が確認されたら、認証機関170の端末を用いて、ステップ804で、ICカード121内で秘密鍵および公開鍵を生成し、データ記憶領域203e(図5)内に秘密鍵501および公開鍵511として格納する。またステップ805で、ICカード121は、生成した公開鍵を認証機関170の端末に送信する。認証機関170の端末では、ステップ806でICカード121から送信された公開鍵を受信し、ステップ807でその公開鍵およびその他の情報を認証機関170の秘密鍵で暗号化して証明書を作成し、ステップ808でその証明書をICカード121に送信する。ICカード121は、ステップ809で、証明書を受信し、自証明書512(図5)として格納する。認証機関170は、ステップ810でユーザ管理情報を更新し、ステップ811で作成したICカード121をサービス提供者100に送付する。サービス提供者100は、ステップ812でそのICカード121を受け取る。

【0077】なお、不図示の処理により、ICカード121には、ICカード申込者に対応するユーザID502、パスワードチェック用データ503、認証機関証明書513、およびICカード番号514が設定されているものとする。

【0078】図8の変形例によれば、認証機関170に秘密鍵が知られてしまうこととなるが、認証機関170が信頼できる機関であれば問題はなく、サービス提供者100が行なう手間が軽減できる。

【0079】図9は、第1の実施の形態において、サービス提供者100およびサービス享受者110、111の間で行なわれるオンラインでの公証サービスの手順を示す流れ図である。同図において、「サービス享受者110」および「サービス享受者111」と記載された下側に並べたブロックは、それぞれ、サービス享受者11

0, 111が使用するサービス享受装置140, 141の端末400内のCPU414がメモリ416内のプログラム(図4)を実行することによる動作である。特に、全体の流れの制御はサービス享受プログラム(416b)で、サービス提供装置130との間でデータの送受信(暗号通信)を行なう際の該データの暗号化と復号化は暗号プログラム(416d)で、サービス提供装置130との間のデータの送受信は通信プログラム(416c)で、それぞれ、行なう。「サービス提供者100」と記載された下側に並べたブロックは、サービス提供者100が使用するサービス提供装置130の端末300内のCPU314がメモリ316内のプログラム(図3)を実行することによる動作であり、特に、全体の流れの制御はサービス提供プログラム(316b)で、サービス享受装置140, 141との間でデータの送受信(暗号通信)を行なう際の該データの暗号化と復号化は暗号プログラム(316d)で、サービス享受装置140, 141との間のデータの送受信は通信プログラム(316c)で、それぞれ、行なう。

【0080】まずステップ900aで、サービス享受者110は、サービス享受装置140により契約内容を暗号化しサービス提供装置130に送信する。サービス提供装置130は、ステップ901aでその契約内容を受信して復号化する。ステップ900b, 901bは、サービス享受者111に関して上記ステップ900a, 901aと同じ処理を、サービス享受装置141とサービス提供装置130との間で行なうものである。次にサービス提供者100は、ステップ902で、サービス享受者110, 111からそれぞれ送られてきた契約内容を照合し、照合がOKであれば、ステップ903で、所定の書式で契約内容その他の情報をまとめた契約情報160(図1)を作成する。そして、ステップ904a, 904bで、サービス提供装置130によりその契約情報160を暗号化しサービス享受装置140, 141にそれぞれ送信する。

【0081】サービス享受者110側では、ステップ905aで、サービス享受装置140により契約情報160を受信し復号化する。サービス享受者110は、ステップ906aでその契約情報160を確認し、確認OKならば、ステップ907aで一者署名付き契約情報161(図1)を作成し、ステップ908aでその一者署名付き契約情報161を暗号化しサービス提供装置130に送信する。サービス提供装置130は、ステップ909aで、その一者署名付き契約情報161を受信し復号化する。ステップ907aの一者署名付き契約情報161の作成手順については、図13で詳しく説明する。

【0082】図10に、ステップ907aで作成した一者署名付き契約情報161の構成を示す。一者署名付き契約情報161は、契約情報160と付属情報1000aと署名1001aとからなる。付属情報1000a

は、サービス享受者110が署名した日時やこの契約に関連する者の名称などこの契約に付随する情報、および署名1001aを確認するために必要なサービス享受者110の証明書や認証機関の証明書からなる。署名1001aは、契約情報160と付属情報1000aとをこの順に連結したデータを所定の方式で圧縮し、得られた圧縮子をサービス享受者110の秘密鍵で暗号化して作成する。

【0083】再び図9に戻って、サービス享受者111側のステップ905b～ステップ908bは、上述したステップ905a～908aの処理をサービス享受者111に対して行なうものである。図11に、サービス享受者111側で作成した一者署名付き契約情報162の構成を示す。図10と同様の構成であるが、付属情報1000bと署名1001bはサービス享受者111に関する情報である。サービス提供装置130は、ステップ909bで、サービス享受者111側の一者署名付き契約情報162を受信し復号化する。

【0084】次に、サービス提供者100は、ステップ910で、サービス提供装置130により三者署名付き契約情報163を作成し外部記憶装置340に保管する。三者署名付き契約情報163の作成手順については、図14で詳しく説明する。

【0085】図12に、三者署名付き契約情報163の構成を示す。三者署名付き契約情報163は、契約情報160と付属情報1000aと付属情報1000bと付属情報1000cと署名1001aと署名1001bと署名1001cとからなる。契約情報160は、一者署名付き契約情報161, 162に含まれている契約情報160である。付属情報1000aと署名1001aは一者署名付き契約情報161に、付属情報1000bと署名1001bは一者署名付き契約情報162に、それぞれ含まれている情報である。付属情報1000cは、サービス提供者100が付けた付属情報である。署名1001cは、契約情報160と付属情報1000a, 1000b, 1000cと署名1001a, 1001bとをこの順に連結したデータを所定の方式で圧縮し、得られた圧縮子をサービス提供者100の秘密鍵で暗号化して作成する。

【0086】このような構成の三者署名付き契約情報163によれば、契約情報160および付属情報1000a, 1000b, 1000cにより、契約内容と契約者の名称や署名日時および公証サービス提供者の名称や署名日時などの契約に関連する各種の情報が分かる。また、署名1001aおよび署名1001bによって、契約した2者であるサービス享受者110および111が契約情報160(および付属情報)に対して確かに署名したものであることが確認できる。また、署名1001cにより、この契約が為されていることを公証サービス提供者100が保証していることが確認できる。契約情

報160と付属情報1000a, 1000b, 1000cと署名1001a, 1001b, 1001cはただ連結してあるだけであるので、分離して署名1001aだけ確認したり、署名1001bだけ確認することもできる。

【0087】再び図9に戻って、ステップ910の後、ステップ911aおよび911bで、サービス提供装置130は三者署名付き契約情報163を暗号化してサービス享受装置140, 141に送信する。サービス享受装置140, 141は、それぞれ、ステップ912a, 912bで三者署名付き契約情報163を受信し復号化する。得られた三者署名付き契約情報163は、サービス享受者110, 111で保管する。

【0088】なお、上述したようにサービス提供装置130とサービス享受装置140, 141との間では暗号通信を行なうが、そのための共通鍵の交換は図9の処理の前処理で行なっているものとする。

【0089】図13は、図9のステップ907aの二者署名付き契約情報161の作成の手順を示す流れ図である。同図において、「サービス享受装置140」と記載された下側に並べたブロックは、サービス享受装置140の端末400内のCPU414がメモリ416内のプログラム(図4)を実行することによる動作であり、特に、全体の流れの制御はサービス享受プログラム(416b)で、ICカード122との間のデータの送受信は端末・ICカード間データ送受信プログラム(416a)で、それぞれ、行なう。「ICカード122」と記載された下側に並べたブロックは、ICカード122内のCPU202がメモリ203内のプログラム(図2)を実行することによる動作であり、特に、全体の流れの制御はICカード制御プログラム(203b)で、サービス享受装置140の端末400との間のデータの送受信は端末・ICカード間データ送受信プログラム(203a)で、署名の生成は署名生成プログラム(203d)で、それぞれ、行なう。

【0090】まずステップ1100で、サービス享受装置140は、証明書出力要求メッセージをICカード122に送信する。ICカード122は、ステップ1101でこの証明書出力要求メッセージを受信し、ステップ1102で自証明書512および認証機関証明書513を送信する。サービス享受装置140は、ステップ1103でこれらの証明書を受信し、ステップ1104で付属情報1000aを生成する。付属情報1000aは、受信した証明書と当該契約に付随する情報(署名日時やサービス享受者110の名称など)とを所定の順序で連結して生成する。次に、ステップ1105で、契約情報160と付属情報1000aとをこの順に連結したデータを圧縮し、圧縮子を生成する。ステップ1106で、圧縮子をICカード122に送信する。

【0091】ICカード122では、ステップ1107

で圧縮子を受信し、ステップ1108でその圧縮子をICカード122内の(サービス享受者110の)秘密鍵501で暗号化して署名1001aを生成する。ステップ1109で、その署名1001aをサービス享受装置140に送信する。サービス享受装置140は、ステップ1110で署名1001aを受信し、ステップ1111で契約情報160と付属情報1000aと署名1001aとをこの順に連結して、図10の二者署名付き契約情報161を生成する。

【0092】なお、ステップ907bの手順も図13と同様である。ただし、ステップ907bでは、サービス享受者111に関する図11の二者署名付き契約情報162を生成する。

【0093】図14は、図9のステップ910の三者署名付き契約情報163の作成の手順を示す流れ図である。同図において、「サービス提供装置130」と記載された下側に並べたブロックは、サービス提供装置130の端末300内のCPU314がメモリ316内のプログラム(図3)を実行することによる動作であり、特に、全体の流れの制御はサービス提供プログラム(316b)で、ICカード121との間のデータの送受信は端末・ICカード間データ送受信プログラム(316a)で、それぞれ、行なう。「ICカード121」と記載された下側に並べたブロックは、ICカード121内のCPU202がメモリ203内のプログラム(図2)を実行することによる動作であり、特に、全体の流れの制御はICカード制御プログラム(203b)で、サービス提供装置130の端末300との間のデータの送受信は端末・ICカード間データ送受信プログラム(203a)で、署名の生成は署名生成プログラム(203d)で、それぞれ、行なう。

【0094】まずステップ1200で、サービス提供装置130は、証明書出力要求メッセージをICカード121に送信する。ICカード121は、ステップ1201でこの証明書出力要求メッセージを受信し、ステップ1202で自証明書512および認証機関証明書513を送信する。サービス提供装置130は、ステップ1203でこれらの証明書を受信し、ステップ1204で付属情報1000cを生成する。付属情報1000cは、受信した証明書と当該契約に付随する情報(署名日時やサービス提供者100の名称など)とを所定の順序で連結して生成する。次に、ステップ1205で、契約情報160と付属情報1000aと付属情報1000bと付属情報1000cと署名1001aと署名1001bとをこの順に連結したデータを圧縮し、圧縮子を生成する。ステップ1206で、圧縮子をICカード121に送信する。

【0095】ICカード121では、ステップ1207で圧縮子を受信し、ステップ1208でその圧縮子をICカード121内の(サービス提供者100の)秘密鍵

501で暗号化して署名1001cを生成する。ステップ1209で、その署名1001cをサービス提供装置130に送信する。サービス提供装置130は、ステップ1210で署名1001cを受信し、ステップ1211で契約情報160と付属情報1000aと付属情報1000bと付属情報1000cと署名1001aと署名1001bと署名1001cとをこの順に連結して、図12の三者署名付き契約情報163を生成する。

【0096】上述の第1の実施の形態の電子公証システムによれば、商取引などを行なう際の契約に係るオンラインでの公証サービスを実現することができる。

【0097】次に、本発明の第2の実施の形態を説明する。第2の実施の形態のシステム構成および処理手順は、上記第1の実施の形態と共通の部分が多いので、共通部分については説明を省略し、以下では第1の実施の形態と異なる部分を中心に説明する。

【0098】上記第1の実施の形態では、サービス享受者110が署名した日時は付属情報1000a(図10)に含まれ、サービス享受者111が署名した日時は付属情報1000b(図11)に含まれ、サービス提供者100が署名した日時は付属情報1000c(図12)に含まれている。しかし、これらの日時データは、サービス享受装置140、141やサービス提供装置130内の内蔵時計に基づくデータであるので、該内蔵時計が誤った時間を示しているときには署名日時が大幅に狂ってしまう。また、サービス享受者などが意識的に不正な日時データを設定することも考えられる。各種の契約においてはどの時点をもって契約が有効になったかが問題になる場合があるので、日時データは正確に設定されるようにしたい。そこで、第2の実施の形態では、時刻管理機関により標準時刻を管理し、付属情報に正確な日時データが設定されるようにした。

【0099】図15は、第2の実施の形態に係る電子公証システムのシステム図である。図15において、図1と共通のものは同じ番号を付し、説明を省略する。図15が図1と異なるのは、ICカード120~123の代わりに内蔵時計を有するICカード1300~1303を用いている点と、時刻管理機関1310が設けられ標準時刻の管理を行なっている点である。これにより、ICカード内で署名を生成する際にICカード内の内蔵時計を時刻管理機関1310の標準時刻に基づいて調整し、調整した内蔵時計の標準時刻に基づいて付属情報の日時データを設定するようにしている。

【0100】図16は、図15のシステムで用いるICカード1300(1301~1303)の内部構成図である。ICカード1300は、図2のICカード120とほぼ同様の構成であるが、内蔵時計1400を備えている。また、図2のICカード制御プログラムの代わりに、別の処理手順のICカード制御プログラムが、メモリ1401の領域1402に格納されている。

【0101】第2の実施の形態において、ICカード発行の手順、認証機関170より証明書153~155を発行してもらう手順、および公証サービスの手順は、図6~図9と同じである。署名付き契約情報161~163の構成は、基本的に図10~図12と同様であるが、各「署名」の直前に「標準時刻」が新たに挿入される点異なる。

【0102】図17は、第2の実施の形態において図9のステップ907aで実行される一者署名付き契約情報の作成の手順を示す流れ図である。ステップ1100~1107の処理は、第1の実施の形態の図13のステップ1100~1107と同じである。第2の実施の形態では、ステップ1107の後、ステップ1500でICカード1302からサービス享受装置140に標準時刻要求メッセージを送信する。サービス享受装置140では、ステップ1501でその標準時刻要求メッセージを受信し、ステップ1502で標準時刻を取得する。標準時刻の取得は、図15に示した時刻管理機関1310にオンラインで標準時刻要求メッセージを送信し、時刻管理機関1310から返送される標準時刻を受信することにより取得する。取得した標準時刻は、ステップ1503で、サービス享受装置140からICカード1302に送信する。ICカード1302では、ステップ1504でその標準時刻を受信し、受信した標準時刻に応じて内蔵時計1400を調整する。

【0103】次にICカード1302は、ステップ1108で、圧縮子(ステップ1107で受信してあるデータ)に内蔵時計1400の標準時刻(この時点の時刻値であり、以下では標準時刻aと呼ぶ)をこの順に連結したデータをICカード1302内の(サービス享受者110の)秘密鍵501で暗号化して署名1001aを生成する。ステップ1109で、標準時刻aと生成した署名1001aとをサービス享受装置140に送信する。サービス享受装置140は、ステップ1110で標準時刻aと署名1001aを受信し、ステップ1111で契約情報160と付属情報1000aと標準時刻aと署名1001aとをこの順に連結して、一者署名付き契約情報161を生成する。

【0104】なお、第2の実施の形態における図9のステップ907bの手順も図17と同様である。ただし、ステップ907bでは、サービス享受者111に関する一者署名付き契約情報162を生成する。一者署名付き契約情報162は、契約情報160と付属情報1000bと標準時刻bと署名1001bとをこの順に連結したデータである。標準時刻bとは、サービス享受者111に関する図17の処理のステップ1108で署名生成したときに用いた標準時刻の時刻値である。

【0105】図18は、第2の実施の形態における図9のステップ910の三者署名付き契約情報の作成の手順を示す流れ図である。ステップ1200~1207の処

理は、第1の実施の形態の図14のステップ1200～1207と同じである。第2の実施の形態では、ステップ1207の後、ステップ1600でICカード1301からサービス提供装置130に標準時刻要求メッセージを送信する。サービス提供装置130では、ステップ1601でその標準時刻要求メッセージを受信し、ステップ1602で標準時刻を取得する。標準時刻の取得は、図15に示した時刻管理機関1310にオンラインで標準時刻要求メッセージを送信し、時刻管理機関1310から返送される標準時刻を受信することにより取得する。取得した標準時刻は、ステップ1603で、サービス提供装置130からICカード1301に送信する。ICカード1301では、ステップ1604でその標準時刻を受信し、受信した標準時刻に応じて内蔵時計1400を調整する。

【0106】次にICカード1301は、ステップ1208で、圧縮子（ステップ1207で受信してあるデータ）に内蔵時計1400の標準時刻（この時点の時刻値であり、以下では標準時刻cと呼ぶ）をこの順に連結したデータをICカード1301内の（サービス提供者1000の）秘密鍵501で暗号化して署名1001cを生成する。ステップ1209で、標準時刻cと生成した署名1001cとをサービス提供装置130に送信する。サービス提供装置130は、ステップ1210で標準時刻cと署名1001cを受信し、ステップ1211で契約情報160と付属情報1000aと付属情報1000bと付属情報1000cと標準時刻aと署名1001aと標準時刻bと署名1001bと標準時刻cと署名1001cとをこの順に連結して、三者署名付き契約情報163を生成する。

【0107】図19は、図18のステップ1602でサービス提供装置130が標準時刻を取得する手順を示す。図17のステップ1502の標準時刻の取得手順も同様である。まずステップ1700で、サービス提供装置130が時刻管理機関1310に標準時刻要求メッセージを送信する。時刻管理機関1310は、ステップ1701で標準時刻要求メッセージを受信し、ステップ1702で標準時刻を送信する。サービス提供装置130は、ステップ1703で標準時刻を受信する。なお、サービス提供装置130やサービス享受装置140、141と時刻管理機関1310との間の通信は、サービス提供装置130、サービス享受装置140、141、および認証機関170のそれぞれの間の通信と同様に、暗号通信で行なうものとする。

【0108】上述の第2の実施の形態の電子公証システムによれば、時刻管理機関1310により管理されている標準時刻を用いて正確な署名日時を契約情報に含めることができるので、契約が成立した時点が明確になり、後に契約の成立時点がいつか問題になったときに対処できる。

【0109】なお、上記第2の実施の形態では、標準時刻a、b、cは付属情報とは別に保持したが、付属情報に含める形式としてもよい。そのためには、付属情報の生成ステップの前で標準時刻を取得し、取得した標準時刻を含めて付属情報を生成するようにすればよい。また、ICカード1300は内蔵時計1400を備えるものとしたが、受信した標準時刻の値をそのまま用いるようにして内蔵時計1400を省略することもできる。

【0110】次に、本発明の第3の実施の形態を説明する。第3の実施の形態のシステム構成および処理手順は、上記第2の実施の形態と共通の部分が多いので、共通部分の説明は省略し、以下では第2の実施の形態と異なる部分を中心に説明する。

【0111】上記第2の実施の形態では、時刻管理機関1310により管理されている標準時刻でICカード1301～1303内の内蔵時計1400を調整し、その標準時刻で署名した日時を正確に記録できるようにした。しかし、ICカード1301～1303内の内蔵時計1400の調整は、基本的に、サービス提供装置130やサービス享受装置140、141を介して行なわれるものである。したがって、サービス提供装置130やサービス享受装置140、141を改造することにより、標準時刻が改変されるおそれがないとはいえない。そこで、第3の実施の形態では、サービス提供装置130やサービス享受装置140、141を介することなく、ICカード内の内蔵時計の調整ができるようにした。

【0112】図20は、第3の実施の形態に係る電子公証システムのシステム図である。図20において、図15と共通のものは同じ番号を付し、説明を省略する。図20が図15と異なるのは、ICカード1300～1303の代わりに内部に無線受信装置を備えたICカード1800～1803を用いている点である。また、不図示であるが、時刻管理機関1310からの標準時刻の送出は無線送信で行ない、直接各ICカード1800～1803で無線受信により標準時刻を取得して内蔵時計の調整を行なうようになっている。

【0113】図21は、図20のシステムで用いるICカード1800（1800～1803）の内部構成図である。ICカード1800は、図16のICカード1300とはほぼ同様の構成であるが、内蔵時計1400に加えて無線受信装置1900を備えている。また、図16のICカード制御プログラムの代わりに、別の処理手順のICカード制御プログラムが、メモリ203の領域1901に格納されている。

【0114】第3の実施の形態において、ICカード発行の手順、認証機関170より証明書153～155を発行してもらう手順、公証サービスの手順、および署名付き契約情報161～163の構成は、上述の第2の実施の形態と同じである。

【0115】図22は、第3の実施の形態において図9のステップ907aで実行される一者署名付き契約情報の作成の手順を示す流れ図である。ステップ1100～1107の処理は、第2の実施の形態の図17のステップ1100～1107と同じである。第3の実施の形態では、ステップ1107の後、ステップ2001でICカード1802内の無線受信装置1900により標準時刻を受信する。時刻管理機関1310では、無線送信装置により標準時刻を常時送信しているので、ステップ2000で送信されている標準時刻をステップ2001で受信すればよい。ICカード1802は、ステップ2002で、受信した標準時刻に応じて内蔵時計1400を調整する。これ以降のステップ1108～1111の処理は、第2の実施の形態の図17のステップ1108～1111と同じである。以上により、サービス享受者110に関する一者署名付き契約情報161を生成する。なお、第3の実施の形態における図9のステップ907bの手順も図22と同様である。ただし、ステップ907bでは、サービス享受者111に関する一者署名付き契約情報162を生成する。

【0116】図23は、第3の実施の形態における図9のステップ910の三者署名付き契約情報の作成の手順を示す流れ図である。ステップ1200～1207の処理は、第2の実施の形態の図18のステップ1200～1207と同じである。第3の実施の形態では、ステップ1207の後、ステップ2101でICカード1801内の無線受信装置1900により標準時刻を受信する。時刻管理機関1310では、無線送信装置により標準時刻を常時送信しているので、ステップ2100で送信されている標準時刻をステップ2101で受信すればよい。ICカード1801は、ステップ2102で、受信した標準時刻に応じて内蔵時計1400を調整する。ステップ1208～1211の処理は、第2の実施の形態の図18のステップ1208～1211と同じである。以上により、三者署名付き契約情報163を生成する。

【0117】上述の第3の実施の形態の電子公証システムによれば、時刻管理機関1310により管理されている標準時刻は、サービス提供装置130やサービス享受装置140、141を介することなく、直接、無線で時刻管理機関1310から各ICカード1801～1803に送られる。したがって、サービス提供装置130やサービス享受装置140、141において日時に改変を施す不正ができなくなり、正確な署名日時を契約情報に含めることができるようになる。

【0118】次に、本発明の第4の実施の形態を説明する。第4の実施の形態のシステム構成および処理手順は、上記第1の実施の形態と共通の部分が多いので、共通部分の説明は省略し、以下では第1の実施の形態と異なる部分を中心に説明する。

【0119】図24は、第4の実施の形態に係る電子公証システムのシステム図である。図24において、図1と共通のものは同じ番号を付し、説明を省略する。図24のが図1と異なるのは、ICカード発行機関180が存在せず、ICカード120～123の代わりにフロッピーディスク2220～2222を用いている点である。なお、フロッピーディスク以外の記憶媒体を用いることも可能である。

【0120】図25は、第4の実施の形態のシステムにおけるサービス提供装置2200の内部構成図である。同図のサービス提供装置2200は、図3に示した第1の実施の形態のサービス提供装置130とはほぼ同じ構成であるが、リーダライタとそのインターフェースを備えていない点、および端末2300内のメモリ2310内の構成が異なる。メモリ2310には、サービス提供プログラムが記憶されている領域316b、通信プログラムが記憶されている領域316c、暗号プログラムが記憶されている領域316d、各種のワーク用データが記憶されるデータ記憶領域316e、暗号鍵生成プログラムが記憶されている領域2311、および署名生成プログラムが記憶されている領域2312が設けられている。領域2311、2312に記憶されている暗号鍵生成プログラムと署名生成プログラムは、第1の実施の形態のICカード120内に備えられている暗号鍵生成プログラムと署名生成プログラムと同様の機能を持つものであるが、第4の実施の形態ではICカードの代わりにフロッピーディスクを用いるので、これらのプログラムはサービス提供装置2200内に備えられている。

【0121】図26は、第4の実施の形態のシステムにおけるサービス享受装置2210の内部構成図である。サービス享受装置2210も同じ構成である。サービス享受装置2210は、図25で説明したサービス提供装置2200とはほぼ同じ構成であるので、説明は省略する。図25の各部に付された300番台および2300番台の番号を400番台および2400番台に読み替えばよい。ただし、図25のサービス提供装置2200は公証サービスを提供する側の装置であるので領域316bにはサービス提供プログラムが格納されているが、図26のサービス享受装置2210は公証サービスを享受する側の装置であるので領域416bにはサービス享受プログラムが格納されている。

【0122】図27は、図24のシステム図におけるフロッピーディスク2220の内容を示すブロック図である。フロッピーディスク2220には、暗号化秘密鍵2500、ユーザID2501、パスワードチェック用データ2502、暗号化公開鍵2503、暗号化自証明書2504、認証機関証明書2505、およびフロッピーディスク番号2506が格納される。これらの情報は、第1の実施の形態の図5で説明したICカード120のデータ記憶領域203eに格納される情報と同様のもの

である。ただし、フロッピーディスクはICカードに比較して簡単に情報が読み出せるので、秘密鍵2500と公開鍵2503と自証明書2504は、このフロッピーディスク2220の正当なユーザのパスワードを鍵として暗号化されている。すなわち、このフロッピーディスク2220を使用する際には、以下の手順で行なうことが要求される。

【0123】このフロッピーディスク2220を使用するとき、ユーザは、ユーザIDとパスワードの入力を装置から要求される。入力されたユーザIDはユーザID 10 2501と照合され、入力されたパスワードは所定の一方方向性の圧縮関数を通してパスワードチェック用データ2502と照合される。照合の結果、正当なユーザであると確認されたら、そのパスワードを端末側のワーク領域に記憶しておく。この後は、暗号化秘密鍵2500、暗号化公開鍵2503、または暗号化自証明書2504を必要に応じて読み出したとき、記憶してあるパスワードでこれらの情報を復号化し、秘密鍵、公開鍵、および自証明書を得る。

【0124】上記ではフロッピーディスク2220について説明したが、フロッピーディスク2221、2222も同様のものである。

【0125】図28は、第4の実施の形態において、サービス提供者100が認証機関170よりフロッピーディスク2220を発行してもらう手順を示す流れ図である。同図において、「サービス提供者100」と記載された下側に並べたブロックはサービス提供者100が行なう動作、「認証機関170」と記載された下側に並べたブロックは認証機関170が行なう動作を示す。

【0126】サービス提供者100は、ステップ2600でフロッピーディスク申込書を作成し、ステップ2601でフロッピーディスク申込書を認証機関170に送付する。認証機関170は、ステップ2602でそのフロッピーディスク申込書を受付け、ステップ603でフロッピーディスク申込書を送付してきた者の身元審査を行なう。身元が確認されたら、ステップ604でユーザ管理情報を更新し、ステップ2603でフロッピーディスク2220をサービス提供者100に送付する。サービス提供者100は、ステップ2606で、フロッピーディスク2220を受け取る。

【0127】なお、認証機関170は、図27で説明したフロッピーディスク2220中のデータのうち、ユーザID2501にはユーザがフロッピーディスク申込書に記載したID（認証機関側でIDを付けることにしてもよい）を設定し、パスワードチェック用データ2502には仮パスワードのチェック用データを設定し、認証機関証明書2505には当該認証機関の公開鍵を設定し、フロッピーディスク番号2506には当該フロッピーディスクの番号を設定して、ユーザに送付する。

【0128】図28ではサービス提供者100が認証機

関170からフロッピーディスク2220を発行してもらう手順を説明したが、サービス享受者110、111が認証機関170からフロッピーディスク2221、2222を発行してもらう手順も同様である。

【0129】図29は、第4の実施の形態において、サービス提供者100が、自フロッピーディスク2220とサービス提供装置2200とを用いて、オンラインで認証機関170より証明書153を発行してもらう手順を示す流れ図である。同図において、「フロッピーディスク2220」と記載された下側に並べたブロックは、フロッピーディスク2220へのアクセスを示す。「サービス提供装置2200」と記載された下側に並べたブロックは、サービス提供装置2200の端末2300内のCPU314がメモリ2310内のプログラム（図25）を実行することによる動作であり、特に、全体の流れの制御はサービス提供プログラム（316b）で、認証機関170の端末との間でメッセージの送受信（暗号通信）を行なう際の該メッセージの暗号化と復号化は暗号プログラム（316d）で、認証機関170の端末との間のメッセージの送受信は通信プログラム（316c）で、暗号鍵の生成は暗号鍵生成プログラム（2311）で、それぞれ、行なう。「認証機関170」と記載された下側に並べたブロックは、認証機関170に備えられた証明書の発行業務を行なう端末における動作を示す。

【0130】サービス提供者100が、サービス提供装置2200に自分のフロッピーディスク2220を挿入し、所定の操作を行なうことで図29の手順が開始する。まずサービス提供装置2200は、ステップ2700でサービス提供者100からの指示に基づいて秘密鍵および公開鍵を生成し、ステップ2701で秘密鍵および公開鍵をパスワードで暗号化してフロッピーディスク2220に書き込む。ステップ2702で、フロッピーディスク2220は、図27に示した所定の領域2500、2503に暗号化秘密鍵と暗号化公開鍵をそれぞれ格納する。

【0131】ステップ703～713の処理は、第1の実施の形態の図7のステップ703～713と同じ処理である。この処理により、サービス提供装置2200は、認証機関170から証明書を取得する。ステップ2703で証明書をパスワードで暗号化し、フロッピーディスク2220に書き込む。フロッピーディスク2220は、ステップ2704で、暗号化証明書を図27に示した所定の領域2504に格納する。

【0132】なお、上記図29では、サービス提供者100が証明書を発行してもらう手順を説明したが、サービス享受者110、111が認証機関170から証明書を発行してもらう手順も同様である。

【0133】この第4の実施の形態において、サービス提供者100およびサービス享受者110、111の間

で行なわれるオンラインでの公証サービスの手順は、第1の実施の形態の図9で説明した手順と同様である。ただし、図9の手順では、サービス享受者110、111側で行なわれるステップ907a、907bの一者署名付き契約情報の作成、およびサービス提供者100側で行なわれるステップ910の三者署名付き契約情報の作成は、図13および図14に示すようにICカードを用いて行なっているが、第4の実施の形態ではICカードの代わりにフロッピーディスクを用いるのでこれらの契約情報の作成手順は異なる。

【0134】図30は、第4の実施の形態において、図9のステップ907aの一者署名付き契約情報の作成の手順を示す流れ図である。サービス享受装置2210は、ステップ2800で、フロッピーディスク2221から暗号化秘密鍵2500と暗号化自証明書2504と認証機関証明書2505とを読み取る。読み取った暗号化秘密鍵2500と暗号化自証明書2504は、パスワードで復号化しておく。次に、ステップ1104で、付属情報1000aを生成する。付属情報1000aは、自証明書や認証機関証明書と当該契約に付随する情報（署名日時やサービス享受者110の名称など）とを所定の順序で連結して生成する。次に、ステップ1105で、契約情報160と付属情報1000aとをこの順に連結したデータを圧縮し、圧縮子を生成する。ステップ2801では、作成した圧縮子を秘密鍵で暗号化して署名1001aを作成する。ステップ1111で、契約情報160と付属情報1000aと署名1001aとをこの順に連結して、図10の一者署名付き契約情報161を生成する。

【0135】なお、ステップ907bの手順も図30と同様である。ただし、ステップ907bでは、サービス享受者111に関する図11の一者署名付き契約情報162を生成する。

【0136】図31は、第4の実施の形態において、図9のステップ910の三者署名付き契約情報の作成の手順を示す流れ図である。サービス提供装置2200は、まずステップ2900で、フロッピーディスク2220から暗号化秘密鍵2500と暗号化自証明書2504と認証機関証明書2505とを読み取る。読み取った暗号化秘密鍵2500と暗号化自証明書2504は、パスワードで復号化しておく。次に、ステップ1204で、付属情報1000cを生成する。付属情報1000cは、自証明書や認証機関証明書と当該契約に付随する情報（署名日時やサービス提供者100の名称など）とを所定の順序で連結して生成する。次に、ステップ1205で、契約情報160と付属情報1000aと付属情報1000bと付属情報1000cと署名1001aと署名1001bとをこの順に連結したデータを圧縮し、圧縮子を生成する。ステップ2901では、作成した圧縮子を秘密鍵で暗号化して署名1001cを作成する。ステ

ップ1211で、契約情報160と付属情報1000aと付属情報1000bと付属情報1000cと署名1001aと署名1001bと署名1001cとをこの順に連結して、図12の三者署名付き契約情報163を生成する。

【0137】上述の第4の実施の形態によれば、安価なフロッピーディスクを用いてオンラインでの公証サービスを実現することができる。

【0138】次に、本発明の第5の実施の形態を説明する。上述の第1～第3の実施の形態ではICカードを用いた公証サービスのシステムを説明したが、第5の実施の形態はそれらの変形例と見ることもできるので、共通部分の説明は省略し、異なる部分のみ説明する。

【0139】第5の実施の形態では、各者の鍵と証明書は、一定期間で変更することを前提とする。これらを一定期間で変更していくことにより、鍵の安全性を高めることができる。しかし、以前に使用していた鍵や証明書を捨ててしまうと、その捨てた鍵を用いて生成した署名を確認・認証できなくなるという不都合がある。そこで、第5の実施の形態では、ICカードに、以前に使用した鍵と証明書を保存しておくようにしている。

【0140】図32は、本発明の第5の実施の形態に係るICカードのデータ記憶領域3000の内容を示す。同図において、図5と同じ情報および領域には同じ番号を付して説明を省略する。このICカードでは、署名履歴3022を記憶する領域を設けておき、署名したときには、どの鍵と証明書をを用いて何時署名したかの履歴を保存するようにする。そして、秘密鍵501、公開鍵511、自証明書512、および認証機関証明書513を新たなものに変更したときには、署名履歴3022を参照して、それまで使用していた秘密鍵501、公開鍵511、自証明書512、および認証機関証明書513を保持しておく必要があったら（それらの鍵や証明書での署名を確認する必要が生じるとされるような場合）、領域3011、3021に退避する。

【0141】第5の実施の形態のICカードによれば、以前に使用していた鍵や証明書を保存しているので、以前の鍵による署名の確認・認証が行なえる。また、署名履歴3022を参照して、その鍵で署名した文書を確認・認証することがなくなったことを確認したら、以前に使用した鍵および証明書を削除すればよい。

【0142】次に、この発明の第6の実施の形態を説明する。上述の各実施の形態のシステムでは、一つの認証機関170がICカードやフロッピーディスクの発行および証明書の発行業務を行なっている。これに対し、第6の実施の形態のシステムは、認証機関を、個人を認証する個人認証局と会員を認証する会員認証局とに分けた点を特徴とするものである。

【0143】図33は、第6の実施の形態のシステム構

成図を示す。ネットワークを介して、会員認証局の端末3310、個人認証局の端末3320、会員Aの端末3330、および会員Bの端末3340が接続されている。ネットワークは、インターネットなどのオープンなネットワーク環境である。

【0144】個人認証局は、個人の公開鍵が真正な本人のものであることを証明し、それを証明する証明書（個人認証書）の発行、保管、および失効の処理を行なう機関である。また、個人認証局は、個人認証書の有効性についての問い合わせに対して応答する。個人認証局への登録は、住民記録に相当するようなものであり、例えば公的機関での運営が想定される。

【0145】図33において、個人認証局の端末3320は、制御モジュール3321、個人登録モジュール3322、個人認証モジュール3323、個人登録抹消モジュール3324、および個人認証書データベース3325を備えている。制御モジュール3321は、申請者の申込みに基づき処理を振り分ける処理を行なう。個人登録モジュール3322は、申請者の申込みに基づき個人の真正さを審査し、個人認証書を発行する処理を行なう。個人認証モジュール3323は、申請者の依頼に基づき、個人認証書の有効性を確認し、その結果を申請者に通知する処理を行なう。個人登録抹消モジュール3324は、申請者の依頼に基づき個人登録を抹消する処理を行なう。個人認証書データベース3325は、各個人の公開鍵その他の情報を保管するデータベースである。

【0146】会員認証局は、ある特定の団体等の会員資格を有する個人の公開鍵が会員資格を有する本人のものであることを証明し、それを証明する会員証の発行、保管、および失効の処理を行なう機関である。また、会員認証局は、会員証の有効性についての問い合わせに対して応答する。上述の個人認証局が住民登録を行なう公的機関のようなものであるのに対し、会員認証局は、例えばクレジットカードの会員であることを証明するような機関である。

【0147】図33において、会員認証局の端末3310は、制御モジュール3311、会員登録モジュール3312、会員認証モジュール3313、会員登録抹消モジュール3314、および会員証データベース3315を備えている。制御モジュール3311は、申請者のネットワークを介した申込みに基づいて処理を振り分ける処理を行なう。会員登録モジュール3312は、申請者の申込みに基づき会員資格を審査し、会員資格があると認めた者に会員証を発行する処理を行なう。会員認証モジュール3313は、申請者の依頼に基づき会員証の有効性を確認し、その結果を申請者に通知する処理を行なう。会員登録抹消モジュール3314は、申請者の依頼に基づき、会員登録を抹消する処理を行なう。会員証データベース3315は、会員資格を有する各個人の公開鍵その他の情報を保管するデータベースである。

【0148】会員Aの端末3330は、情報交換モジュール3331、およびICカード入出力モジュール3332を備えている。情報交換モジュール3331は、ネットワークを介して他の端末と情報をやり取りする各種の処理を行なう。ICカード入出力モジュール3332は、個人認証局や会員認証局から発行されたICカードとの間で各種の情報を入出力するためのモジュールである。会員Bの端末3340は、情報交換モジュール3341およびICカード入出力モジュール3342を備えている。これらは会員Aの端末3330に備えられているものと同様のモジュールである。

【0149】図34に、会員証データベース3315の内部構造を示す。会員証データベース3315は、各会員ごとに、会員証番号、会員名、個人認証書番号、有効期間、会員の公開鍵、および予備の情報を格納するデータベースである。有効期間は、開始日時と終了日時とからなる。会員の公開鍵は、鍵のアルゴリズム、および鍵のビット列からなる。図示しないが、個人認証局の端末3320に備えられている個人認証書データベース3325も同様の構造を有するものであり、各個人ごとに、個人名、個人認証書番号、有効期間、個人の公開鍵、および予備の情報を格納している。

【0150】図35は、図33のシステムによる会員登録の手順を示す流れ図である。まず申込者は、個人認証局に対して個人認証書の発行・送付依頼を行なう。個人認証局は、登録の申請者が確かにその者であるか否か身元を審査し、身元が確認できたら個人認証書を発行・送付する。個人認証書は、住民登録の証明書に相当するようなものであり、具体的には、その個人の公開鍵とその公開鍵がその個人のものであることを証明する個人認証局の証明書とを含むデジタルデータである。通常、個人認証局での身元審査は対面審査によると考えられるので、申込者からの個人認証書の発行・送付依頼や個人認証局からの個人認証書の送付は、申込者が個人認証局に出向いて行なう。ただし、身元審査を行なう手段があれば、ネットワークを介してオンラインで行なってもよい。個人認証書はデジタルデータであるので、個人認証書を受け取った個人は、ICカードやフロッピーディスクなど任意の記憶装置に個人認証書を格納して管理する。ここでは、ICカードに個人認証書を格納して管理するものとする。

【0151】次に申込者は、以下の手順で会員登録を行なう。以下、会員証登録の通知までの手順は、特に指摘した処理を除き、ネットワークを介してオンラインで行なうものである。

【0152】まず、申込者が申込者の端末（3330や3340）で会員登録申込書送付依頼を指示する操作を行なうと、申込者の端末は、会員認証局の端末3310に対して会員登録申込書の送付依頼を行なう。会員認証局の端末3310は、その依頼に応じて会員登録申込書

を送付する。会員登録申込書を受信した申込者の端末は、その会員登録申込書をディスプレイに表示する。申込者がディスプレイ上で会員登録申込書に所定の事項を書き込み、その会員登録申込書の送付を端末に指示すると、申込者の端末は、書き込み済みの会員登録申込書に個人認証書を添付して、会員認証局の端末3310に送付する。会員認証局の端末3310は、その申込書と個人認証書を受け取ったら、申込受付の応答を申込者の端末に返す。

【0153】次に会員認証局の端末3310は、送付されてきた個人認証書の有効性の確認依頼を個人認証局の端末3320に対して行なう。個人認証局の端末3320は、その個人認証書の有効性を確認し、確認結果を会員認証局の端末3310に送付する。会員認証局の端末3310でその確認結果を受けたら、会員認証局は、その確認結果およびその他の情報に基づいて会員資格の審査を行ない、会員資格有りと判断されたときは、鍵生成ソフトが内蔵されているICカードを申込者に郵送する。

【0154】申込者は、申込者の端末にそのICカードを挿入してそのICカード中で会員証を作成する。具体的には、会員として使用する公開鍵と秘密鍵のペアを生成し、秘密鍵はICカード内の外部出力禁止領域に格納し、公開鍵はICカード内の外部出力許可領域に格納するとともに、生成した公開鍵を含む申込者に関する所定の情報を所定のフォーマットでまとめたデータである会員証をICカード内に作成するということである。申込者は、申込者の端末を使用して、作成した会員証に個人認証書を添付して会員認証局の端末3310に送付する。

【0155】会員認証局の端末3310は、送付された個人認証書の有効性の確認依頼を個人認証局の端末3320に対して行ない、個人認証局の端末3320は、その個人認証書の有効性を確認する。確認結果は会員認証局の端末3310に送付される。個人認証書の有効性が確認されたら、会員認証局の端末3310は、会員証の登録を行ない申込者に会員証登録の通知を行なう。具体的には、その申込者の公開鍵を含む会員証が確かにその者のものであることを証明する証明書を申込者に送付するということである。申込者の端末は、送られてきた証明書

をICカードに格納する。以上によりこの申込者の会員登録が行なわれた。

【0156】なお、上述の図35の手順は、申込者が個人認証局から個人認証書を送付してもらうまでのフェーズ、申込者が会員認証局に会員登録申込書の送付依頼を出してから申込受付の応答を受領するまでのフェーズ、会員認証局が会員登録申込書を受けてからICカードを申込者に郵送するまでのフェーズ、申込者がICカードを受け取ってから会員証を作成し個人認証書を添付して会員認証局に送付するまでのフェーズ、および会員認

局が申込者から会員証と個人認証書の送付を受けてから会員登録の通知を出すまでのフェーズに分かれており、これら各フェーズ間にはタイムラグがある。そのため、そのタイムラグの間に個人認証書が無効になる場合も考えられるので、会員認証局から個人認証局への個人認証書の確認は2回行なっている。ただし、個人認証書の確認を1回で済ませてもよい。その場合は、申込者がICカード内で会員証を作成して会員認証局の端末3310に送信したら（個人認証書の添付は不要）、会員認証局の端末3310で、個人認証書の有効性の確認を行なうことなく、会員証の登録を行ない申込者に会員証登録の通知を行なうようにすればよい。

【0157】図36は、会員登録抹消の手順を示す流れ図である。申込者が申込者の端末（3330や3340）で会員登録抹消処理を指示すると、申込者の端末は、個人認証書と会員証とを添付して会員登録の抹消の申込みを会員認証局の端末3310に対して送信する。会員認証局の端末3310は、送られてきた個人認証書の有効性の確認依頼を個人認証局の端末3320に対して発行する。個人認証局の端末3320は、その個人認証書の有効性を確認し、その確認結果を会員認証局の端末3310に送付する。会員認証局の端末3310は、その確認結果を受けて、個人認証書が有効なものであれば会員証の有効性を確認した上で、当該会員の会員登録を抹消し、会員者登録抹消の通知を申込者の端末に対して行なう。

【0158】以上の手順によれば、個人認証書を確認することにより本人からの登録抹消依頼であることが確認できる。これにより、個人認証書を入手した第3者が悪用しようとしたとき（会員登録を抹消しようとしたとき）、本人が個人認証局に個人認証書の紛失を届けていれば、個人認証書の有効性を確認する際に紛失したものであることが判明するので、悪用を防止することができる。同様に、会員証の確認も行なっているので、会員証を入手した第3者が悪用しようとしたとき（会員登録を抹消しようとしたとき）、本人が会員認証局に会員証の紛失を届けていれば、会員証の有効性を確認する際に紛失したものであることが判明するので、悪用を防止することができる。この例では、個人認証書と会員証は別のICカードに格納しているが、個人認証書のICカードを紛失したときは個人認証局に、会員証のICカードを紛失したときは会員認証局に、それぞれ届け出ることになるので、何れか一方を紛失しても個人認証書の確認または会員証の確認のどちらかでチェックされ悪用は防止できる。

【0159】図37は、会員Aと会員Bとの間で何らかの取引を行なうとき相手を確認するための手順を示す。まず、会員Aの端末3330から個人認証書と会員証の送付依頼を、会員Bの端末3340に対して送信する。この送付依頼に応じて、会員Bの端末3340は、会員

Bの個人認証書と会員証を会員Aの端末3330に送信する。会員Aの端末3330は、受信した会員Bの会員証と個人認証書とを会員認証局の端末3310に送信して、会員Bの有効性の確認依頼を行なう。これを受けて、会員認証局の端末3310は、会員Bの会員証の有効性を確認するとともに、個人認証局の端末3320に対して個人認証書の有効性の確認依頼を送信する。個人認証局の端末3320は、この依頼に基づき個人認証書の有効性を確認し、確認結果を会員認証局の端末3310に送付する。会員認証局の端末3310は、会員証の

【0160】以上により、会員Aは、会員Bの会員証と個人認証書の両方の有効性を確認して、会員Bの真正性を確認することができる。会員Bが会員Aの真正性を確認するのも同様に行なえばよい。

【0161】図38は、図33の会員認証局の端末3310の制御モジュール3311の処理手順を示すフローチャートである。まずステップ3801で、会員からの依頼内容（ネットワークを介して会員の端末3330や3340から送信されてきた依頼内容）を判別し、その依頼内容に応じて分岐する。依頼内容が会員登録であるときは、ステップ3702で会員登録モジュール3312により会員登録の処理を行なう。依頼内容が会員認証であるときは、ステップ3703で会員認証モジュール3313により会員認証の処理を行なう。依頼内容が会員登録抹消であるときは、ステップ3704で会員登録抹消モジュール3314により会員登録抹消の処理を行なう。

【0162】図39は、図38のステップ3802の会員登録モジュール3312による処理手順を示すフローチャートである。このフローチャートは、図35の手順のうち、申込者が会員認証局に会員登録申込書の送付依頼を出してから会員認証局が会員資格の審査結果を出すまでの、会員認証局の端末3310が行なう処理を示すものである。まずステップ3901で、申込者の端末3330や3340から送信された会員登録申込書送付依頼を受け、ステップ3902で、その申込者の端末へ会員登録申込書を送信する。会員登録申込書は所定フォームの電子的な文書であり、申込者はその会員登録申込書に各種の事項を書き込んだ後、その会員登録申込書と自分の個人認証書とを会員認証局の端末3310に送信してくるので、ステップ3903でそれらを受付ける。会員登録申込書と個人認証書とを受け付け、ステップ3904で、申込者の端末に申し込み受付を応答する。

【0163】次に、会員認証局の端末3310は、ステップ3905で、個人認証局の端末3320に対し、当該申込者の個人認証書の有効性の確認を依頼する。個人認証局の端末3320は、その依頼に基づいて当該個人認証書の有効性を確認し、確認結果を会員認証局の端末3310に送信するので、会員認証局の端末3310で

は、ステップ3306でその確認結果を受領し、当該個人認証書が有効であるか無効であるか判別する。無効であるときは、ステップ3909で会員資格が無い旨を申込者の端末に通知し処理を終了する。当該個人認証書が有効なものであるときは、ステップ3907で会員資格を審査する。会員資格有りの場合は、ステップ3908で、会員登録を実施して良い旨を表示し処理を終了する。会員資格が無い場合は、ステップ3909に進む。

【0164】図39の処理により会員登録を実施して良い場合は、図35で説明したように鍵生成ソフト内蔵のICカードを当該申込者に郵送する。申込者は、ICカード中で会員証を作成し、会員証に個人認証書を添付して会員認証局の端末3310に送付する。

【0165】図40は、申込者から送られてくる会員証と個人認証書を受け付けるところから会員証登録の通知を行なうまでの、会員認証局の端末3310の、処理手順を示すフローチャートである。まずステップ4001で、申込者の端末（3330や3340）から送信されてくる会員証と個人認証書を受け付ける。次にステップ4002で、個人認証局の端末3320に対し、当該個人認証書の有効性の確認を依頼する。個人認証局の端末3320は、その個人認証書の有効性を確認し、確認結果を会員認証局の端末3310に送信してくるので、会員認証局の端末3310では、ステップ4003でその確認結果を受領し、有効か無効かを判別する。当該個人認証書が有効なものであるときは、ステップ4004で会員証データベース3315に当該申込者の各種の情報を登録し、ステップ4005で申込者に会員証登録完了の旨を通知して処理を終了する。会員証登録完了の通知には、会員資格を有するこの申込者の公開鍵が確かに本人のものであることを証明する証明書（具体的には、公開鍵を含む所定の情報を会員認証局の秘密鍵で暗号化したもの）を含む会員証が含まれている。ステップ4003で当該個人認証書が無効なものであるときは、ステップ4006で、会員登録ができない旨を当該申込者に通知して処理を終了する。

【0166】図41は、図38のステップ3804の会員登録抹消モジュール3314による処理手順を示すフローチャートである。このフローチャートは、図36で会員認証局の端末3310が行なう処理を示すものである。まずステップ4101で、会員の端末（3330や3340）から送信されてくるその会員本人の個人認証書と会員証と会員登録の抹消の申込みを受け付ける。次にステップ4102で、個人認証局3320に対し、当該個人認証書の有効性の確認を依頼する。個人認証局の端末3320は、この依頼を受けて当該個人認証書の有効性を確認し確認結果を送信してくるので、会員認証局3310では、ステップ4103でその確認結果を受領し、有効か無効かを判別する。当該個人認証書が有効な

ものであるときは、ステップ4104で、会員証の有効性を確認した上で、会員証データベース3315中の当該会員の情報を無効とする。また、ステップ4105で当該申込者に対し会員登録抹消を通知して、処理を終了する。ステップ4103で当該個人認証書が無効なものであったときは、ステップ4106で、会員登録抹消不可の旨を当該申込者に通知して処理を終了する。

【0167】図42は、図38のステップ3803の会員認証モジュール3313による処理手順を示すフローチャートである。このフローチャートは、図37で説明した会員認証局の端末3310が行なう処理である。まずステップ4201で、会員の端末から送信されてくる有効性を確認したい対象者の個人認証書と会員証を受け付ける。次にステップ4202で、会員証データベース3315を参照し、当該会員証の有効性を確認する。当該会員証が有効なものであるときは、ステップ4203で、個人認証局3320に対し当該個人認証書の有効性の確認を依頼する。個人認証局の端末3320は、その依頼を受けて個人認証書の有効性を確認し、確認結果を送信してくるので、会員認証局の端末3310は、ステップ4204でその確認結果を受領し、有効か無効かを判別する。当該個人認証書が有効なものであるときは、ステップ4205で、その申込者に対し会員証が有効である旨を通知して、処理を終了する。ステップ4204で当該個人認証書が無効なものであるときは、ステップ4206で、その申込者に対して会員証が無効である旨を通知し、処理を終了する。

【0168】以上説明した第6の実施の形態によれば、会員認証局は、会員登録処理時に個人認証局に対し個人認証書の有効性の確認を行なってもらうことにより、個人の識別を非対面で行なうことができる。住民登録に相当するような個人認証は公的機関がその役割を担うことが想定され、そこでは対面してその個人の身元確認を行なうと考えられる。一方、各種の団体などで会員登録を行なう際には、個人認証局に照会しさえすればその個人の身元確認ができるので、非対面で会員登録を行なうことができ、会員登録の処理の手間が省ける。この際、公的機関が保管すべき個人のプライバシー情報は見ることなく、会員としての審査に必要な情報のみを個人認証局から会員認証局へ送付することにより、各個人のプライバシーを侵害することなく身元確認が行なえる。また、会員AおよびB間で各種の取引を行なうときの確認は、会員証の確認と個人認証書の確認の両方を行なうようにしているので、取引を行なおうとしている相手方の真正性が確度高く確認できる。会員認証書と個人認証書とを別々のICカードなどで保有しているので、どちらかを紛失したときには、会員認証局または個人認証局に届け出れば、悪用の可能性は少ない。

【0169】次に、この発明の第7の実施の形態を説明する。上記各実施の形態で説明したように各個人の公開

鍵を所定の認証機関に登録して証明書を発行してもらう場合、登録の手間を軽減するため、複数の個人の公開鍵の登録をまとめて認証機関に依頼することが考えられる。例えば、企業内でその企業に勤務する者の公開鍵の登録を、その企業内の責任者がまとめて認証機関に依頼するような場合である。この場合、その企業に勤務する者が登録を申し出た公開鍵に対し、その企業内の責任者が、故意にその公開鍵に不正を加えたり偶発的に公開鍵に不正が加えられることが考えられる。

【0170】そこで、第7の実施の形態では、ある責任者が複数の登録申請者の公開鍵の登録をまとめて行なう場合に、その責任者の不正を防止するため、以下のような手順で登録を行なう。以下では、企業D内で公開鍵の登録を申請する申請者Aの公開鍵を、登録責任者Bが、取りまとめて認証局（認証機関）Cに登録を依頼する場合を例に説明する。まず、登録の申請者Aは、認証局Cの公開鍵で自分の公開鍵（登録を申請する公開鍵）を暗号化し、これを登録責任者Bに渡す。登録責任者Bは、申請者Aから登録を申請された公開鍵に電子署名して、認証局Cに送付する。認証局Cでは、登録責任者Bによる電子署名により途中で改竄されていないことを確認した後、認証局Cの秘密鍵で登録申請者Aの公開鍵を取り出し、登録申請者Aの証明書を作成し、この証明書を企業Dの公開鍵で暗号化した後、企業Dの登録責任者Bあるいは登録申請者Aに送付する。登録責任者Bに送付された場合は、当該証明書が登録申請者Aに必ず渡されるという保障が無いため、認証局Cは、当該証明書を企業Dの公開鍵以外に登録申請者Aの公開鍵で暗号化して送付するようにしても良い。

【0171】図43は、第7の実施の形態における公開鍵登録の手順を示すフローチャートである。ステップ4301～4304は登録申請者Aの処理フロー、ステップ4305、4306および4313、4314は登録責任者Bの処理フロー、ステップ4307～4312は認証局Cの処理フローを、それぞれ示す。

【0172】まず登録申請者Aは、ステップ4310で公開鍵を生成し、ステップ4302で認証局Cの公開鍵を入手する。次にステップ4303で認証局Cの公開鍵で自分の公開鍵を暗号化し、ステップ4304で暗号化した自分の公開鍵を登録責任者Bに渡してその公開鍵の登録を申請する。図示しないが、他の登録申請者も同様に暗号化した公開鍵を登録責任者Bに渡し登録を申請するが、処理は同様であるので以下では登録申請者Aのみに着目して説明する。

【0173】登録責任者Bは、ステップ4305で、受付けた登録申請者Aの暗号化公開鍵およびその他の必要な情報をまとめて証明書発行依頼書を作成し、自分の秘密鍵で電子署名を行ない、ステップ4306でその電子署名付き証明書発行依頼書を認証局Cに送付する。

【0174】認証局Cでは、ステップ4307で、登録

責任者Bから送付された電子署名付き証明書発行依頼書の署名を確認し、当該証明書発行依頼書が確かに登録責任者Bから送られたものであってかつ改竄されていないかどうか判別する。登録責任者Bからであってかつ改竄されていないときは、ステップ4309で、当該証明書発行依頼書に含まれている暗号化された登録申請者Aの公開鍵を認証局Cの秘密鍵で復号する。ステップ4310で、登録申請者Aの公開鍵の証明書を作成する。ステップ4311でその証明書を企業Dの公開鍵で暗号化し、ステップ4312で認証書を発行し、ステップ4313に進む。ステップ4307で証明書発行依頼書が登録責任者Bからのもので無い場合、または証明書発行依頼書が改竄されていたときは、ステップ4308で、登録責任者Bにその旨を通知し改竄されていた登録申請者の暗号化公開鍵を破棄する。なお、図43のフローチャートでは、ステップ4308で改竄されている暗号化公開鍵のみを破棄し、正当なものと思われる暗号化公開鍵については、ステップ4309以降の処理を行なうこととしている。ただし、一つでも登録申請者の公開鍵に改竄が加えられていると判別されたときは、ステップ4308の後、処理を終了してもよい。

【0175】登録責任者Bは、ステップ4313で、認証局Cから送付された認証書を受け取り、企業Dの秘密鍵で復号して登録申請者Aの公開鍵の証明書を得、ステップ4314でその証明書を登録申請者Aに配布する。

【0176】この第7の実施の形態によれば、企業D内において公開鍵の登録を登録責任者Bが取りまとめる際に、偶発的あるいは故意に未登録の公開鍵に不正が加えられることを防ぎ、確かに登録責任者B（企業D）により依頼されたことを保証し、また認証局Cからの証明書を確実に企業Dに送付することが可能となる。企業D内において公開鍵の登録をまとめて行なう場合は、登録申請者の審査のためその上司・人事・総務などの各部門を経由して最終的に登録責任者Bが認証局Cに証明書の発行依頼をすることが考えられるが、この審査過程での偶発的あるいは故意に行なわれる不正も防ぐことができる。認証局Cが証明書を送付する際に、企業Dの公開鍵以外に登録申請者Aの公開鍵で暗号化して送付するようにすれば、証明書を安全・確実に登録申請者Aに渡せる。

【0177】

【発明の効果】以上説明したように、本発明によれば、オープンなネットワーク環境において電子商取引を行なう際に必要とされる認証・公証サービス（電子情報署名・保管サービス）が実際に実現できる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係る電子公証システムのシステム図である。

【図2】本発明の第1の実施の形態におけるICカードの内部構成図である。

【図3】本発明の第1の実施の形態におけるサービス提供装置の内部構成図である。

【図4】本発明の第1の実施の形態におけるサービス享受装置の内部構成図である。

【図5】本発明の第1の実施の形態におけるICカード内のデータ記憶領域の中身を示すブロック図である。

【図6】本発明の第1の実施の形態において、サービス提供者が認証機関よりICカードを発行してもらう手順を示す流れ図である。

【図7】本発明の第1の実施の形態において、サービス提供者が、自ICカードとサービス提供装置とを用いて認証機関より証明書を発行してもらう手順を示す流れ図である。

【図8】本発明の第1の実施の形態の変形例であり、サービス提供者が認証機関より証明書格納済みのICカードを発行してもらう手順を示す流れ図である。

【図9】本発明の第1の実施の形態において、サービス提供者およびサービス享受者の間で行われるサービス処理の全体手順を示す流れ図である。

【図10】本発明の第1の実施の形態における一者署名付き契約情報の一例である。

【図11】本発明の第1の実施の形態における一者署名付き契約情報のもう一つの例である。

【図12】本発明の第1の実施の形態における三者署名付き契約情報の一例である。

【図13】本発明の第1の実施の形態において、サービス享受装置とICカードとが連動して一者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図14】本発明の第1の実施の形態において、サービス提供装置とICカードとが連動して三者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図15】本発明の第2の実施の形態に係る電子公証システムのシステム図である。

【図16】本発明の第2の実施の形態におけるICカードの内部構成図である。

【図17】本発明の第2の実施の形態において、サービス享受装置とICカードとが連動して一者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図18】本発明の第2の実施の形態において、サービス提供装置とICカードとが連動して三者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図19】本発明の第2の実施の形態において、サービス提供装置が時刻管理機関から標準時刻を取得する手順を示す流れ図である。

【図20】本発明の第3の実施の形態に係る電子公証システムのシステム図である。

【図21】本発明の第3の実施の形態におけるICカードの内部構成図である。

【図22】本発明の第3の実施の形態において、サービス享受装置とICカードと時刻管理機関とが連動して一

者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図23】本発明の第3の実施の形態において、サービス提供装置とICカードと時刻管理機関とが連動して三者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図24】本発明の第4の実施の形態に係る電子公証システムのシステム図である。

【図25】本発明の第4の実施の形態におけるサービス提供装置の内部構成図である。

【図26】本発明の第4の実施の形態におけるサービス享受装置の内部構成図である。

【図27】本発明の第4の実施の形態におけるフロッピーディスクの中身を示すブロック図である。

【図28】本発明の第4の実施の形態において、サービス提供者が認証機関よりフロッピーディスクを発行してもらう手順を示す流れ図である。

【図29】本発明の第4の実施の形態において、サービス提供者が、自フロッピーディスクとサービス提供装置とを用いて認証機関より証明書を発行してもらう手順を示す流れ図である。

【図30】本発明の第4の実施の形態において、サービス享受装置が一者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図31】本発明の第4の実施の形態において、サービス提供装置が三者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図32】本発明の第5の実施の形態におけるICカードの内部構成図である。

【図33】本発明の第6の実施の形態のシステム構成図である。

【図34】本発明の第6の実施の形態における会員証データベースの内部構造図である。

*

*【図35】本発明の第6の実施の形態における会員登録の手順を示す流れ図である。

【図36】本発明の第6の実施の形態における会員登録抹消の手順を示す流れ図である。

【図37】本発明の第6の実施の形態における会員間で何らかの取引を行なうとき相手を確認するための手順を示す流れ図である。

【図38】本発明の第6の実施の形態における会員認証局の端末の制御モジュールの処理手順を示す流れ図である。

【図39】本発明の第6の実施の形態における会員認証局の端末の会員登録モジュールの処理手順（その1）を示す流れ図である。

【図40】本発明の第6の実施の形態における会員認証局の端末の会員登録モジュールの処理手順（その2）を示す流れ図である。

【図41】本発明の第6の実施の形態における会員認証局の端末の会員登録抹消モジュールの処理手順を示す流れ図である。

【図42】本発明の第6の実施の形態における会員認証局の端末の会員認証モジュールの処理手順を示す流れ図である。

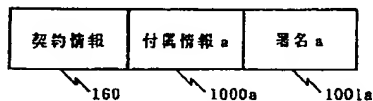
【図43】本発明の第7の実施の形態における公開鍵登録の手順を示す流れ図である。

【符号の説明】

100…サービス提供者、110、111…サービス享受者、120、121、122、123…ICカード、130…サービス提供装置、140、141…サービス享受装置、150、151、152…公開鍵、153、154、155…証明書、160…契約情報、161、162…一者署名付き契約情報、163…三者署名付き契約情報、170…認証機関、180…通信網。

【図10】

一者署名付き契約情報 161



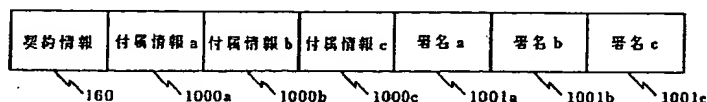
【図11】

一者署名付き契約情報 162

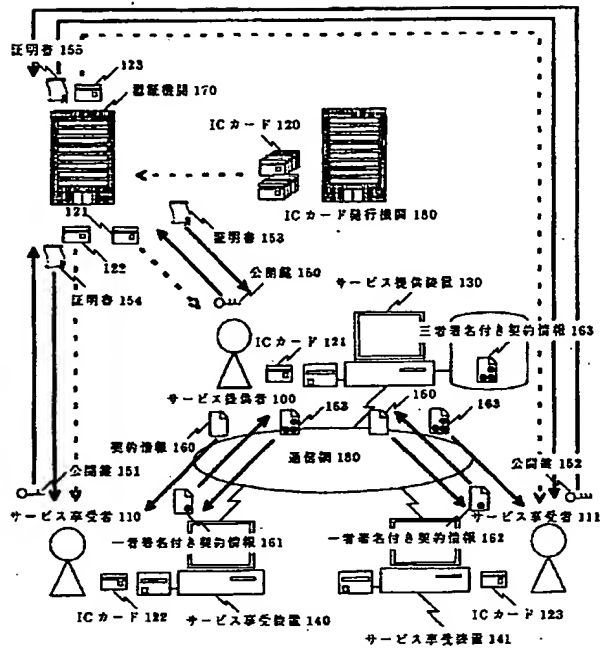


【図12】

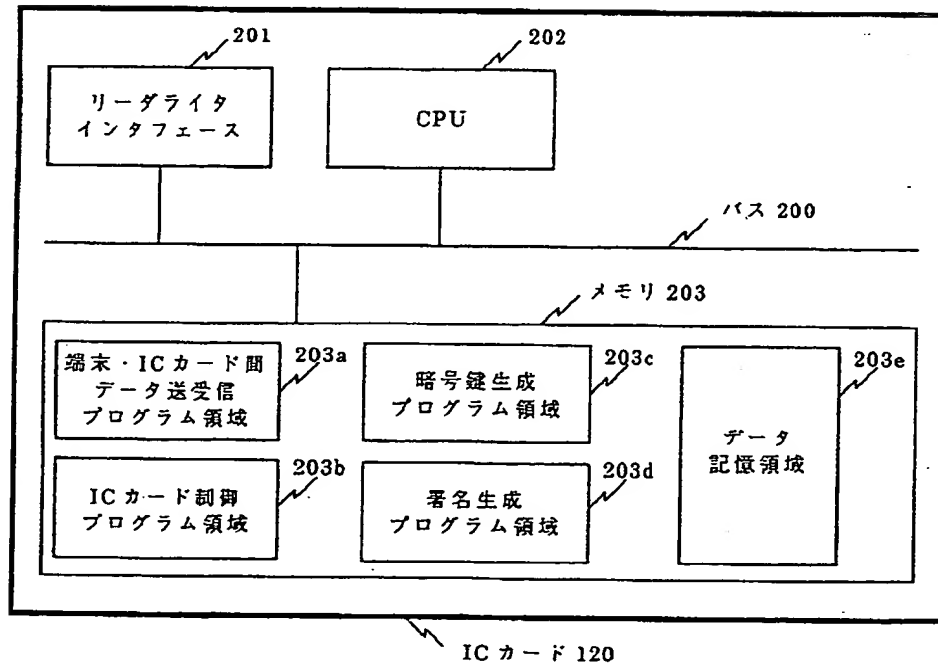
三者署名付き契約情報 163



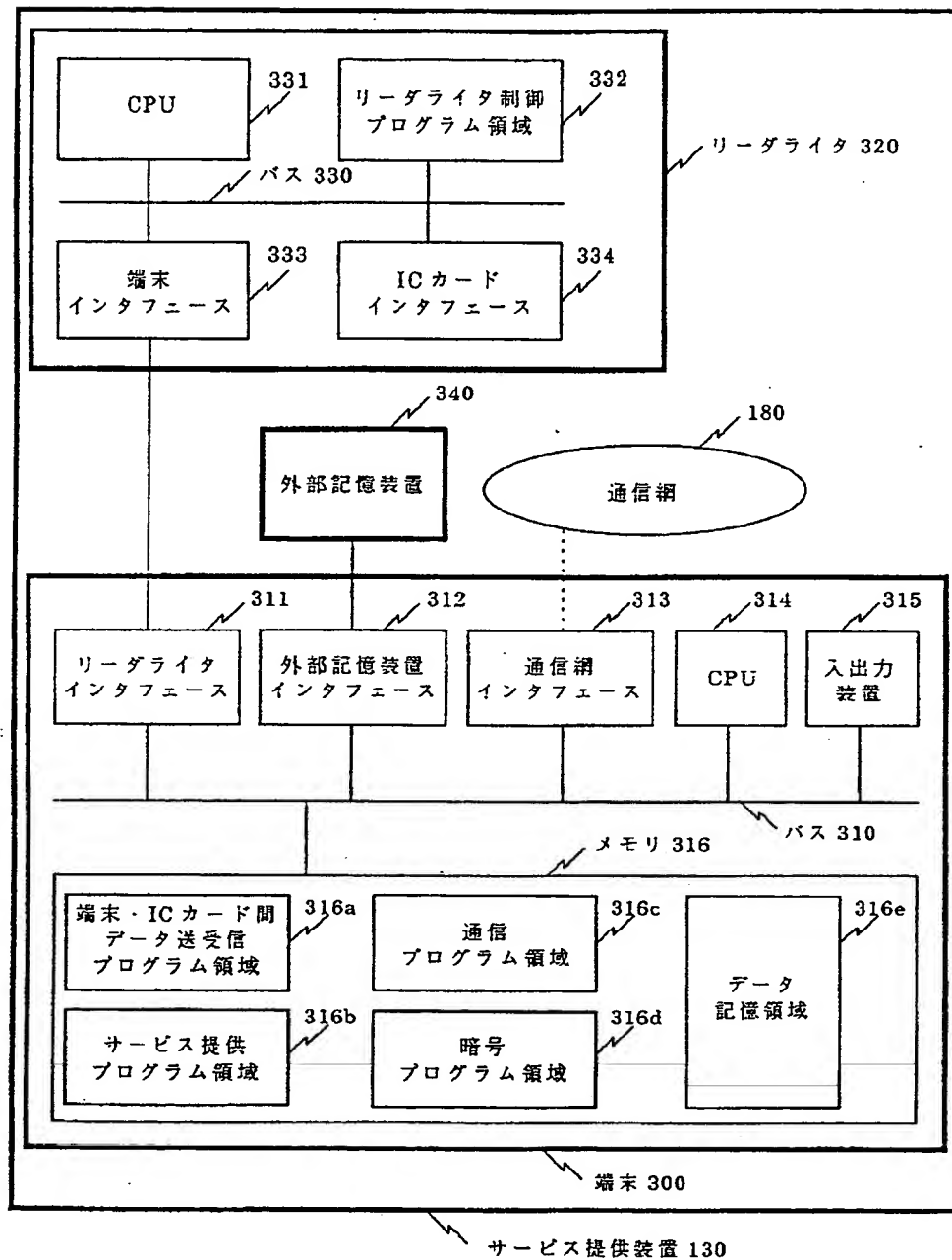
【図1】



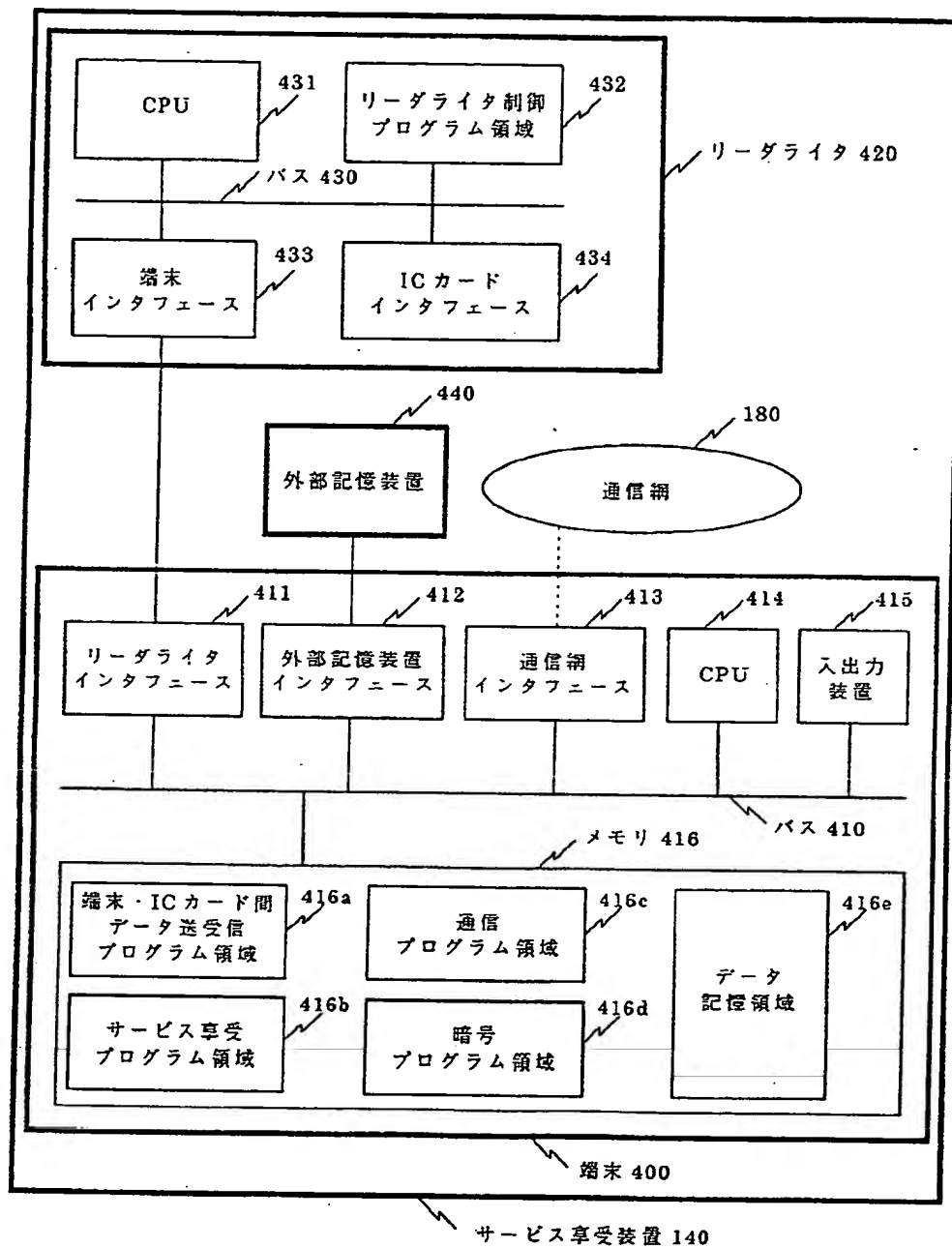
【図2】



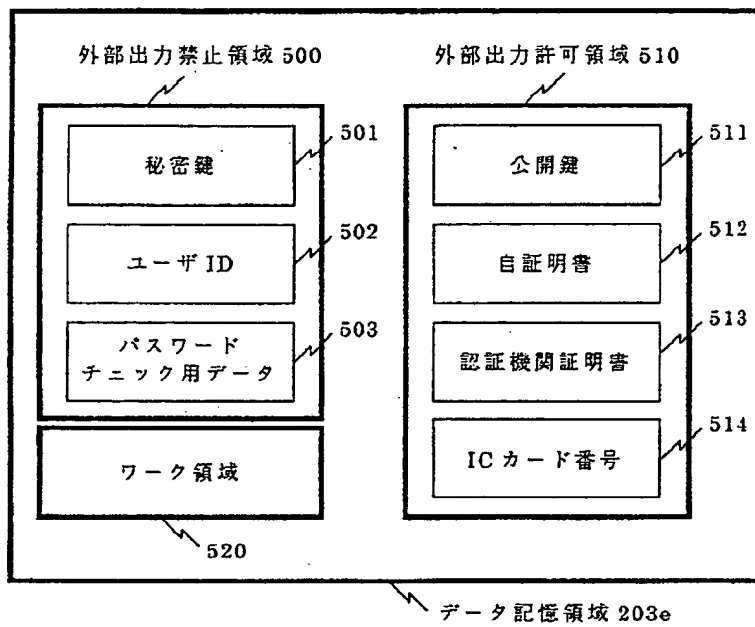
【図3】



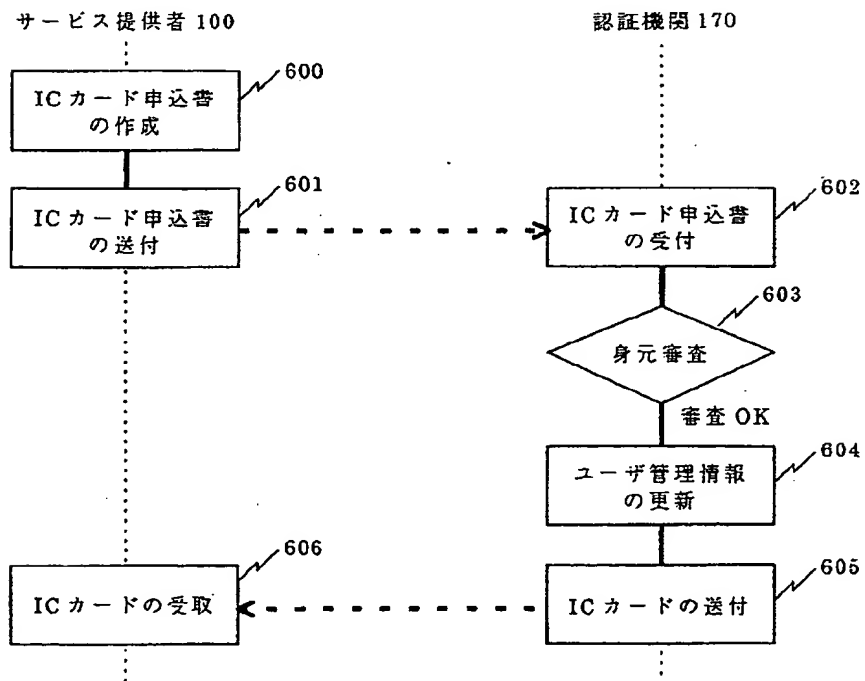
【図4】



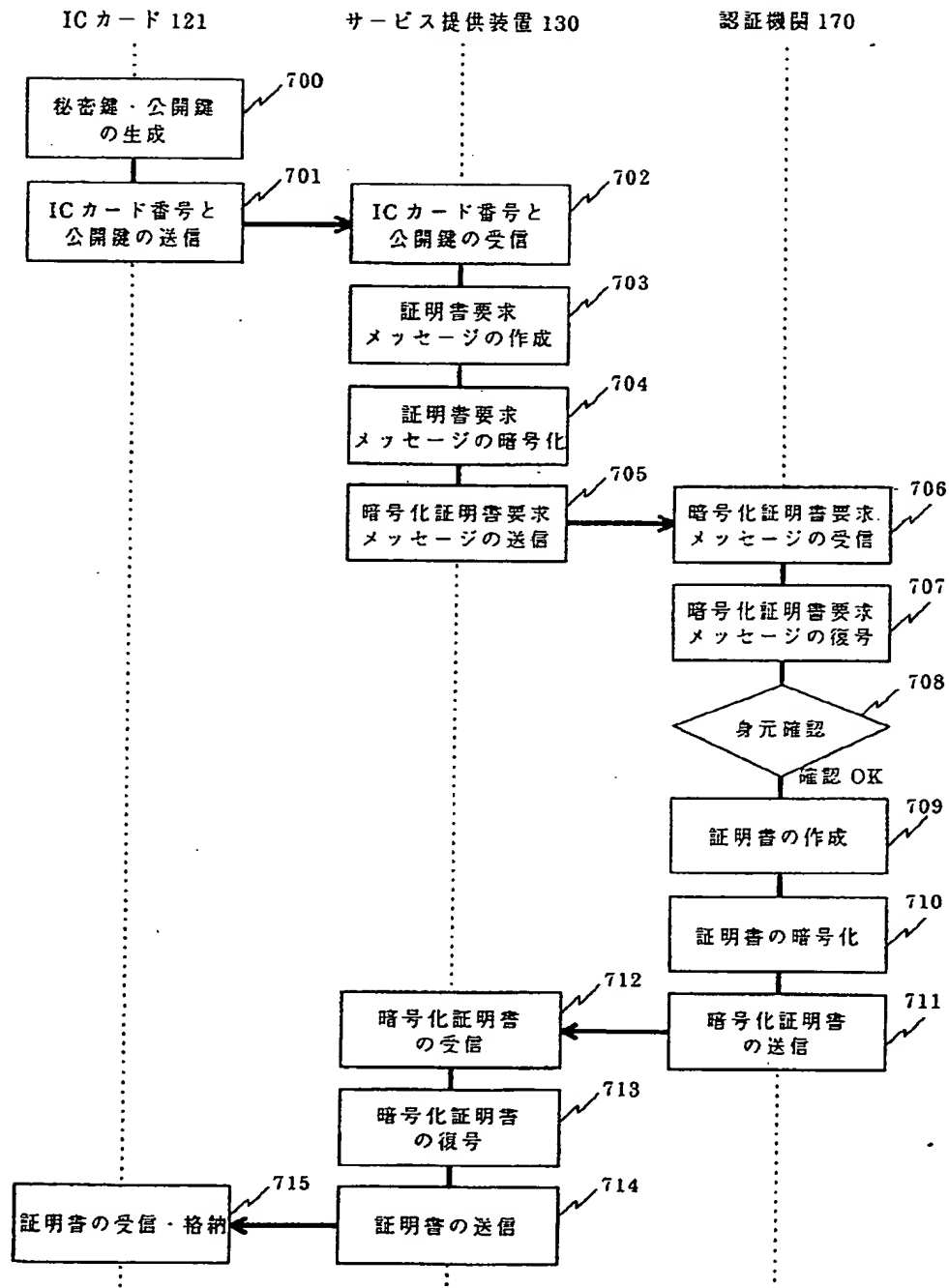
【図5】



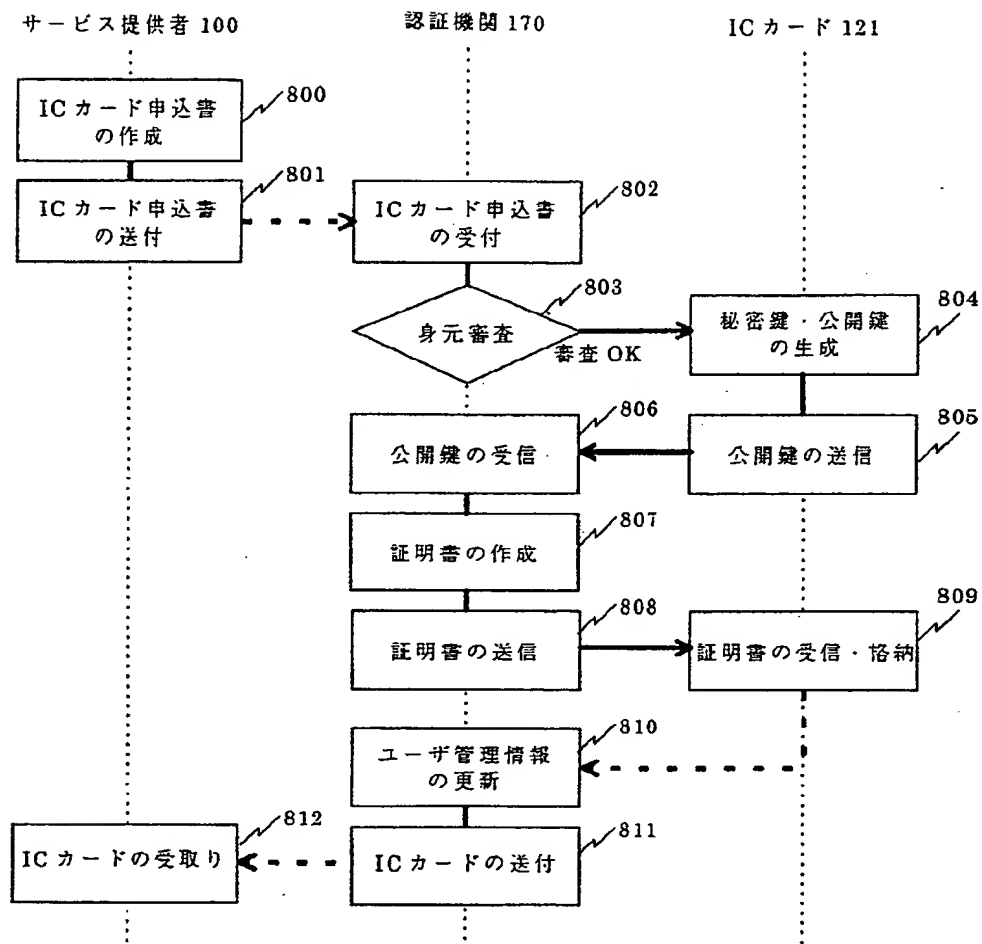
【図6】



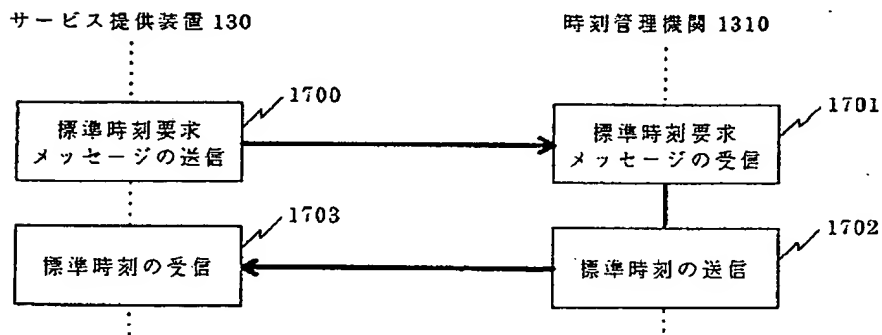
【図7】



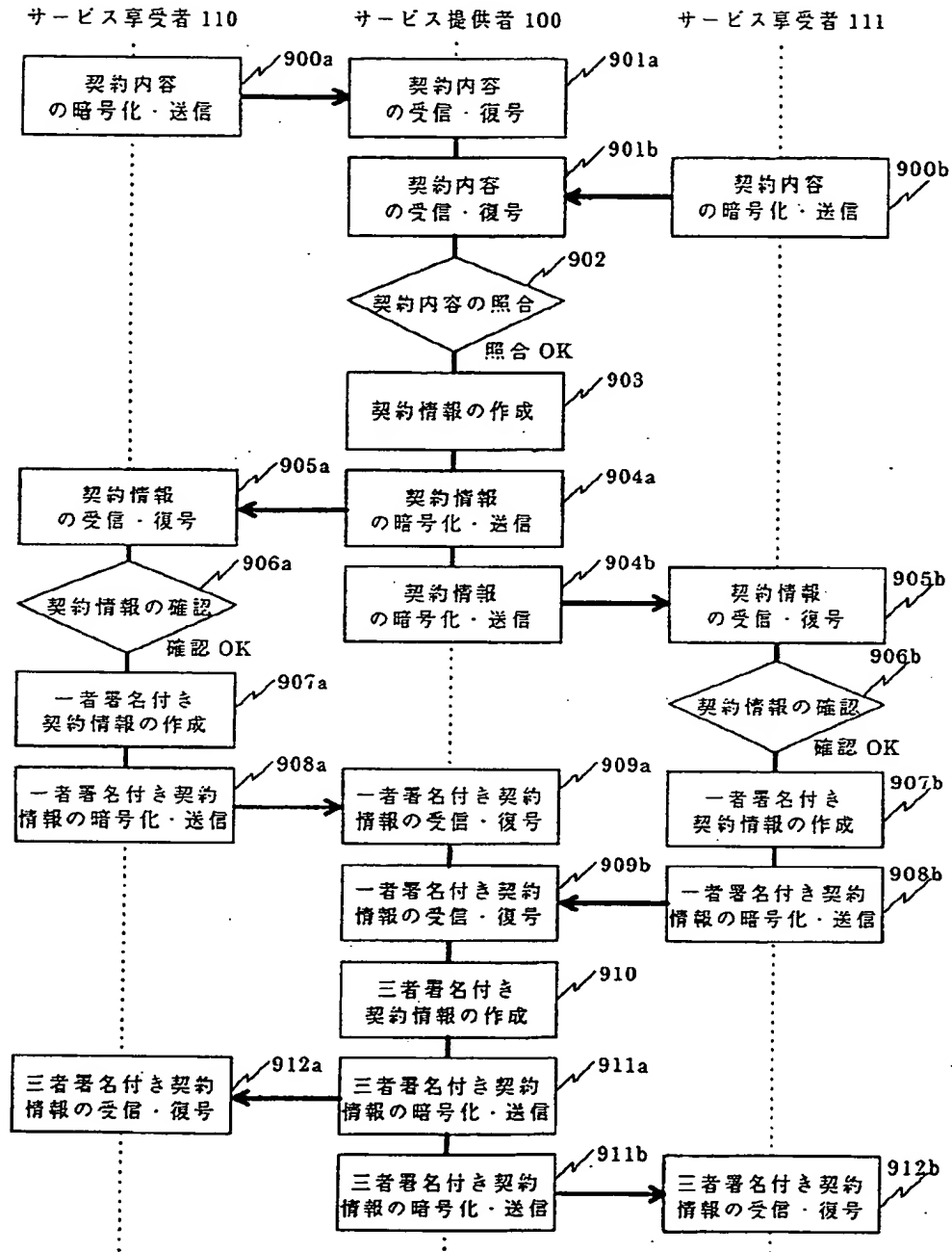
【図8】



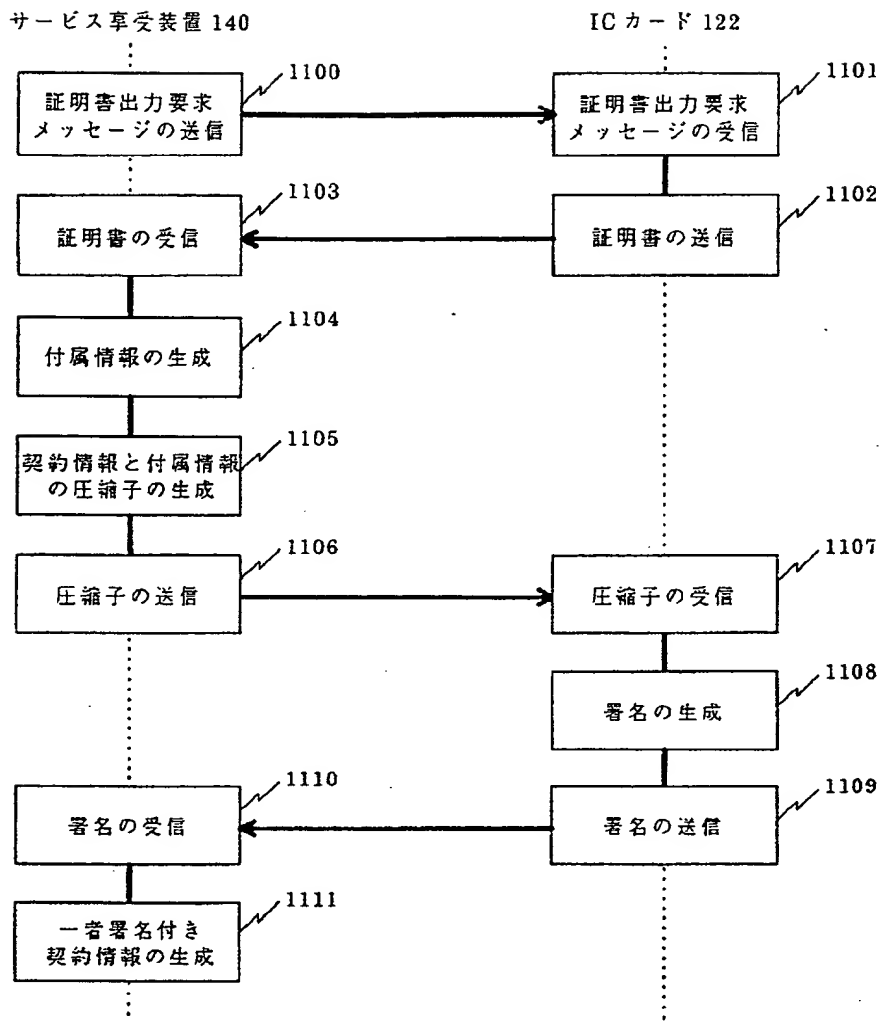
【図19】



【図9】



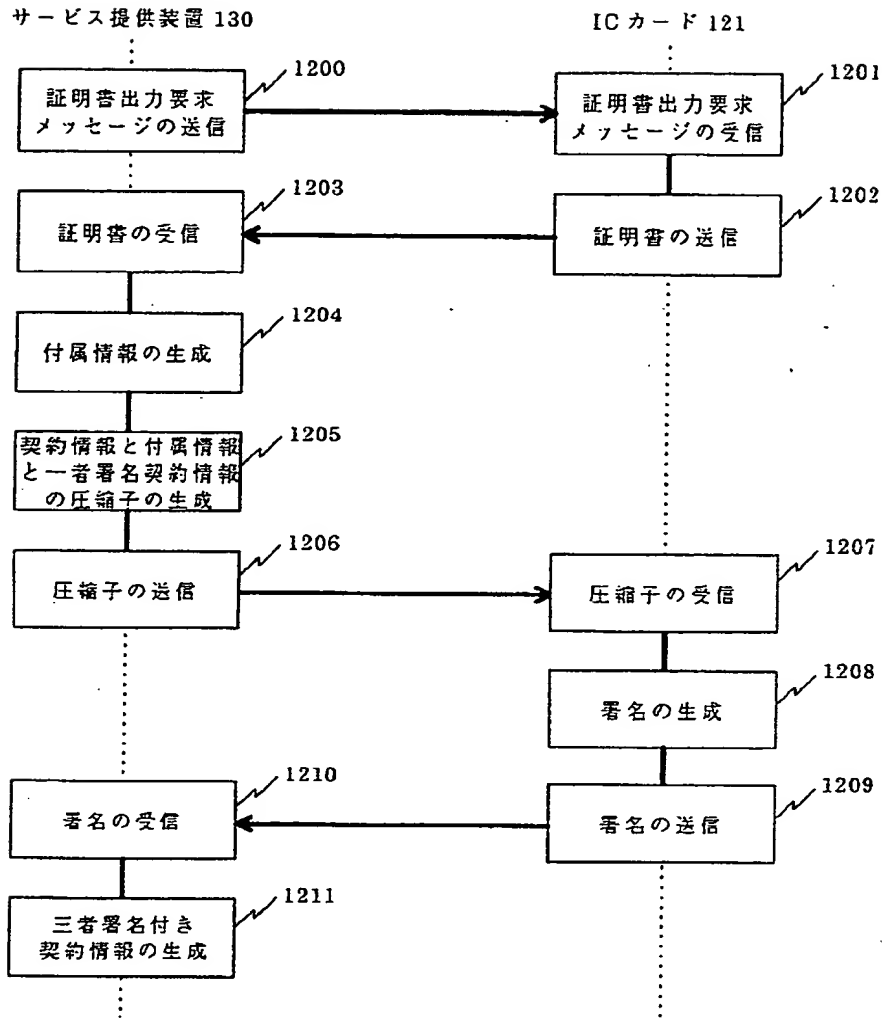
【図13】



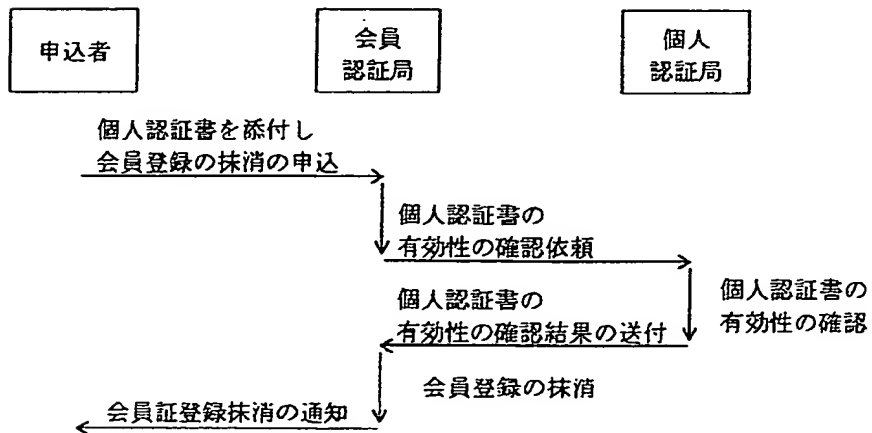
【図34】

会員証番号	会員名	個人認証書 番号	有効期間		会員の公開鍵		予備
			開始日時	終了日時	鍵の アルゴリズム	鍵(ビット列)	

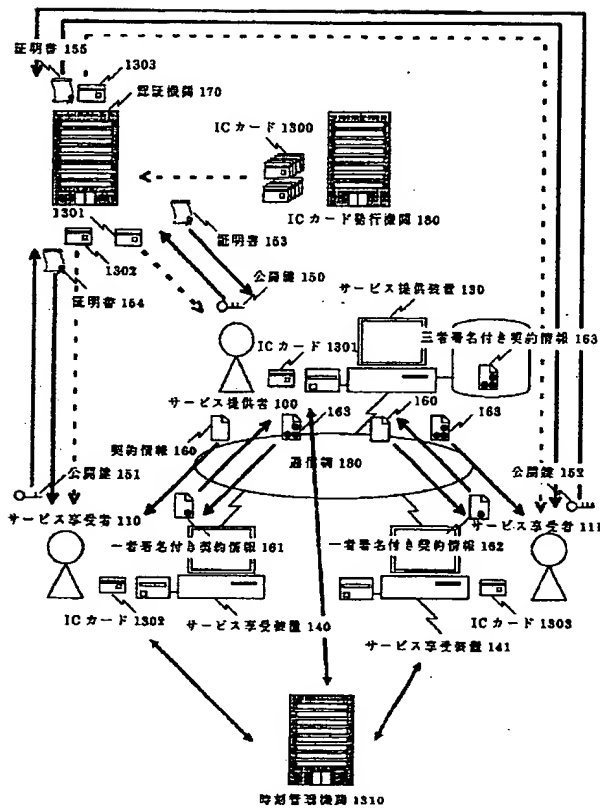
【図14】



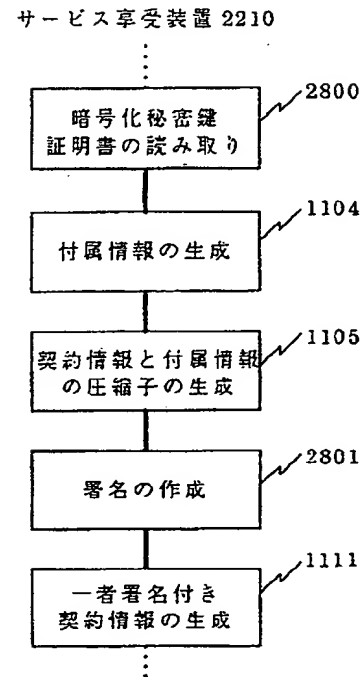
【図36】



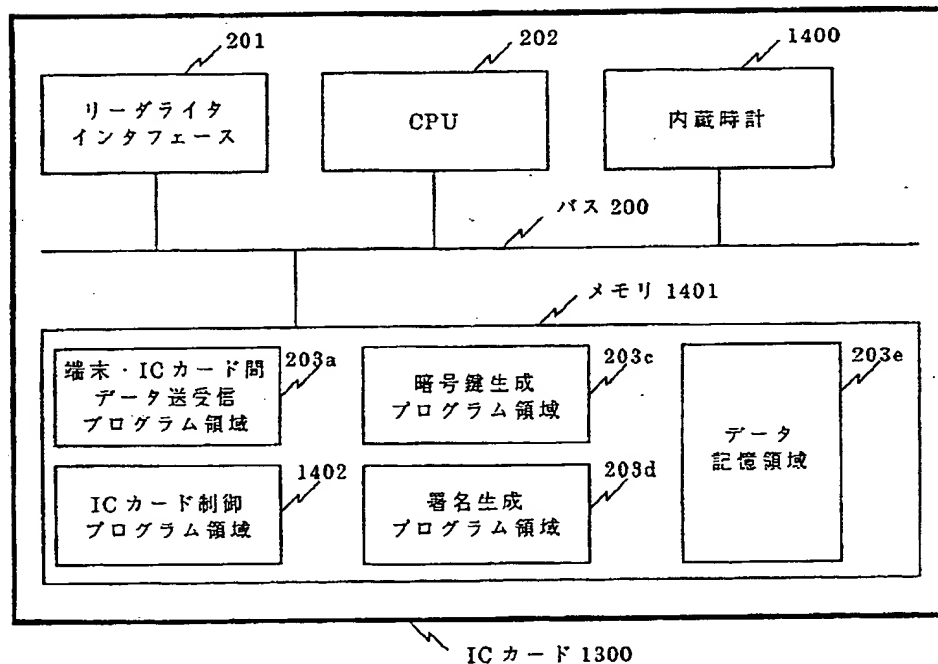
【図15】



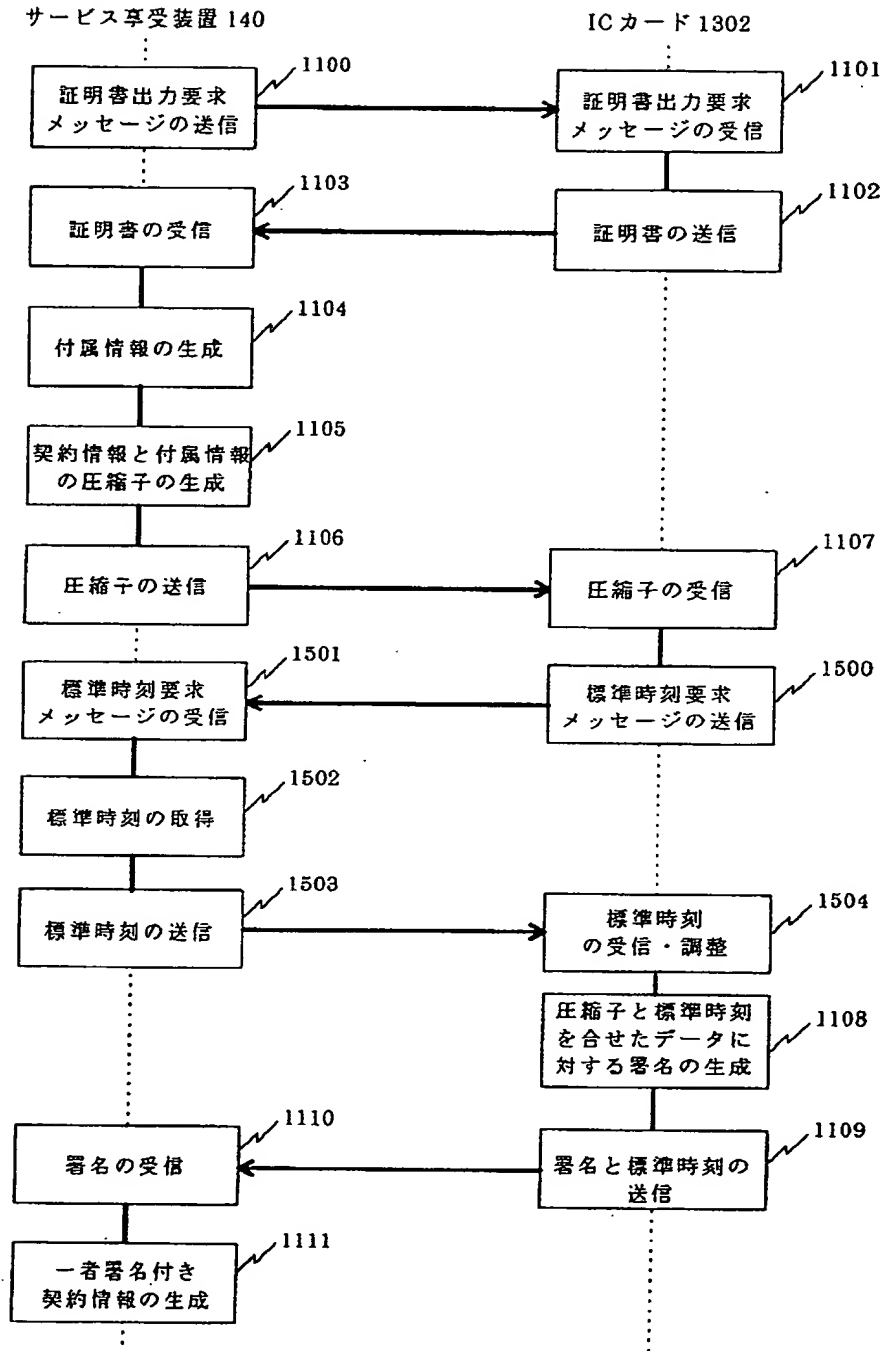
【図30】



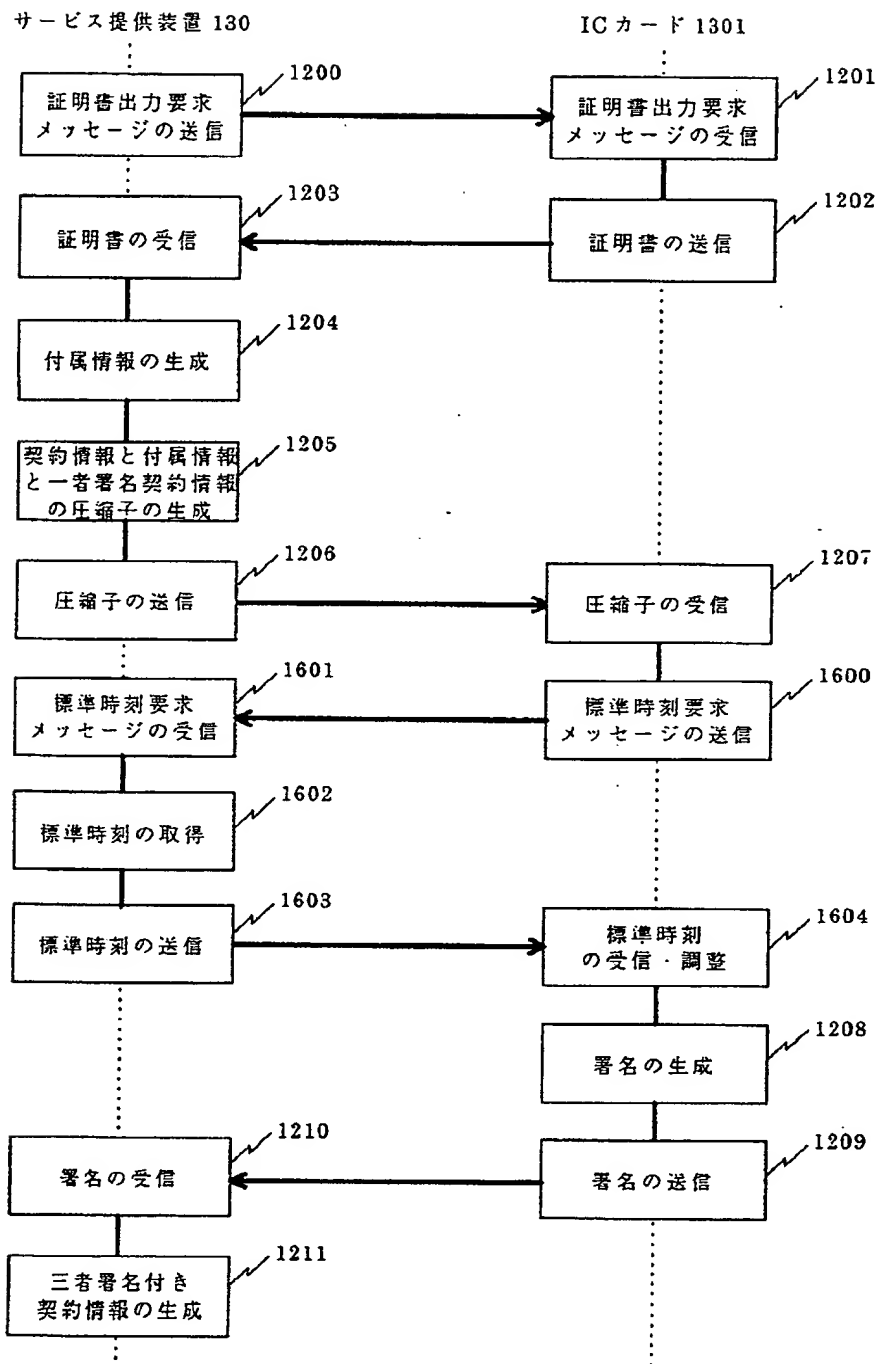
【図16】



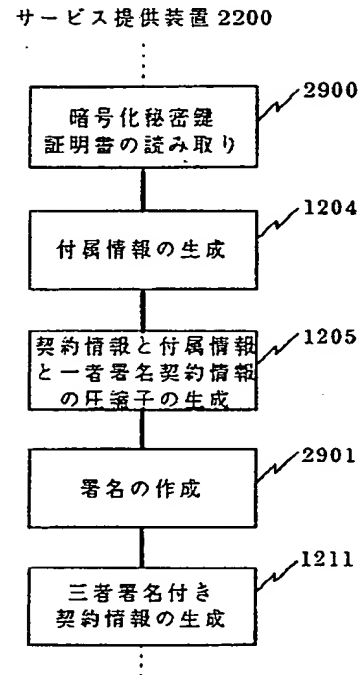
【図17】



【図18】



【図 3 1】



The diagram illustrates the architecture of the IC card system, showing the internal components of the IC card and its connection to an external system.

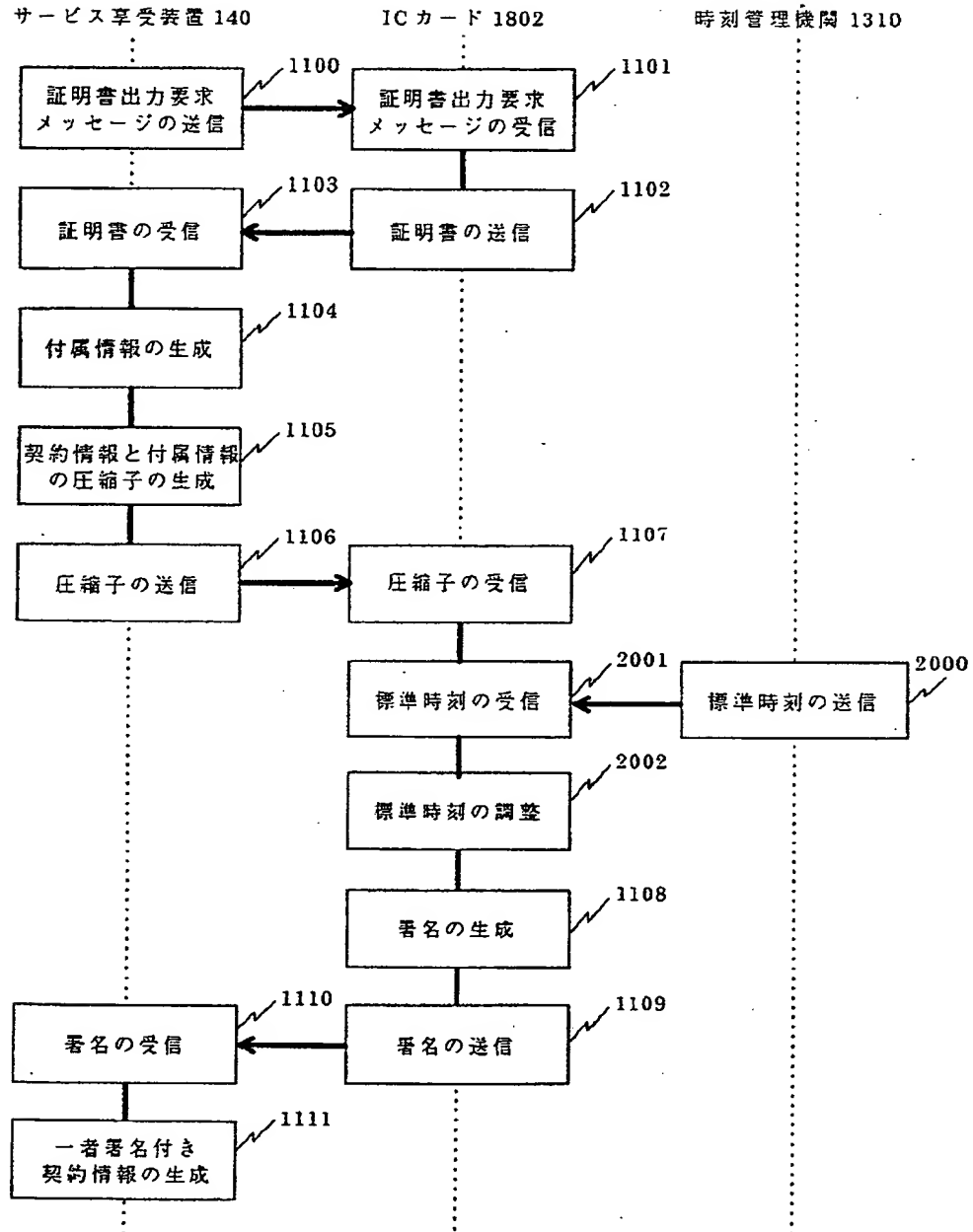
IC Card Internal Components:

- 201:** リーダライタインタフェース (Reader/Writer Interface)
- 202:** CPU (Central Processing Unit)
- 1400:** 内蔵時計 (Built-in Clock)
- 1900:** 無線受信装置 (Wireless Reception Device)
- バス 200:** Bus connecting the internal components.
- メモリ 203:** Memory block containing:
 - 203a:** 端末・ICカード間データ送受信プログラム領域 (Terminal/IC Card Data Transmission/Reception Program Area)
 - 203c:** 暗号鍵生成プログラム領域 (Cryptographic Key Generation Program Area)
 - 203d:** 署名生成プログラム領域 (Signature Generation Program Area)
 - 203e:** データ記憶領域 (Data Storage Area)
- 1901:** ICカード制御プログラム領域 (IC Card Control Program Area)

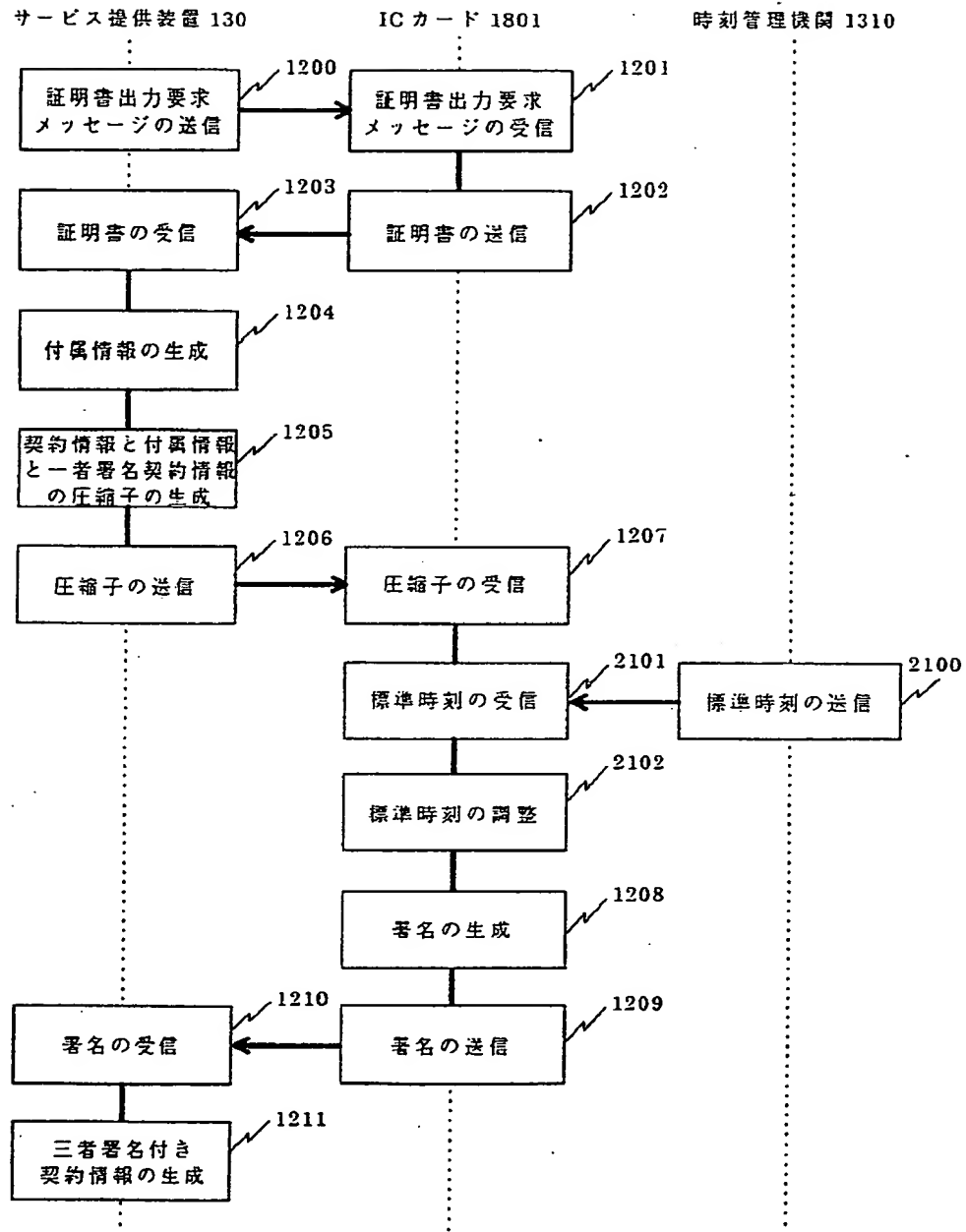
External System:

- 1800:** ICカード (IC Card) - The external system component connected to the IC card.

【図22】



【図23】



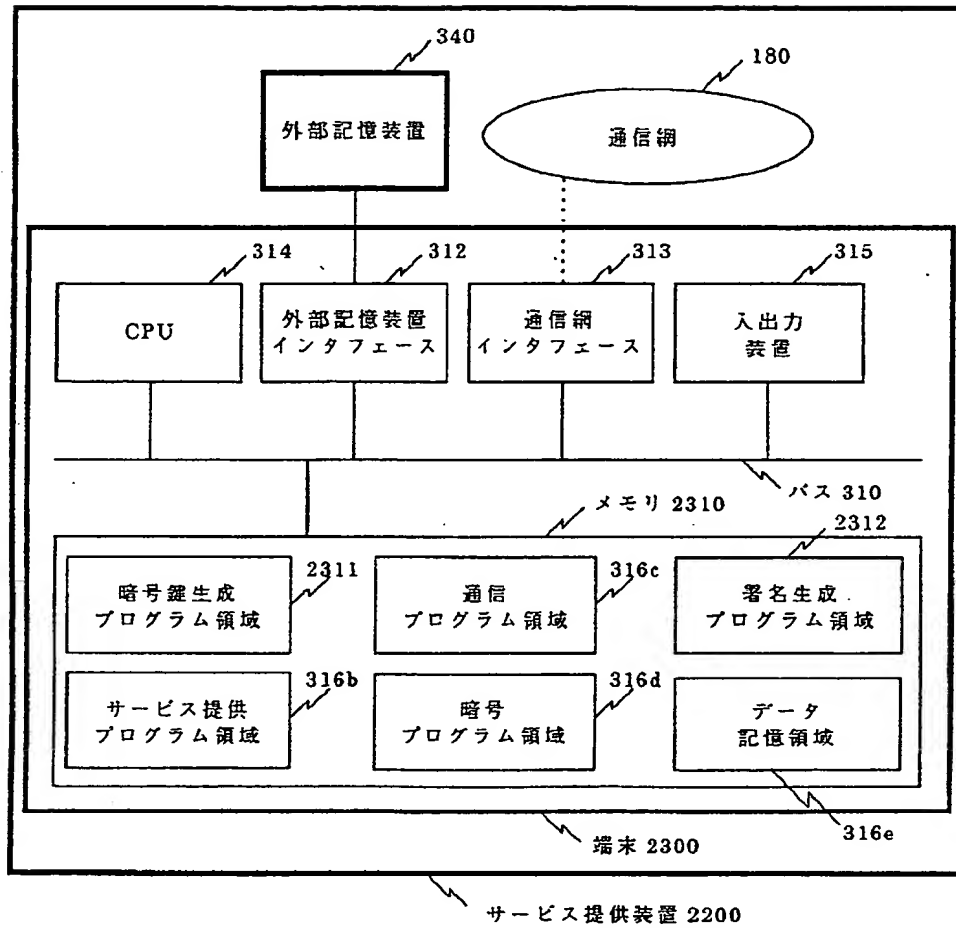
The diagram illustrates a system architecture enclosed in a dashed rectangular boundary. At the top left, a '証明書155' (Certificate 155) is shown next to a '認証機関170' (Authentication Authority 170). Below them are two databases labeled '2223' and '2220'. To the right, another database is labeled '2221'. In the center, there's a '証明書154' (Certificate 154) and a '公開鍵150' (Public Key 150). On the far right, a 'サービス提供装置2200' (Service Provision Device 2200) is connected to a 'フロッピーディスク2220' (Floppy Disk 2220) and a '三省署名付き契約情報162' (Contract Information 162 with three ministries' names). Below these, a 'サービス提供者100' (Service Provider 100) is connected to a '契約情報160' (Contract Information 160) and a '三省署名付き契約情報161' (Contract Information 161 with three ministries' names). A central '通信網180' (Communication Network 180) connects several components. At the bottom, there are two 'サービス受取装置2210' (Service Reception Device 2210) and 'サービス享受装置2211' (Service Enjoyment Device 2211), each with its own 'フロッピーディスク2221' (Floppy Disk 2221). On the right side, a '公同鍵152' (Common Key 152) is shown near a 'サービス受取者111' (Service Receiver 111). The diagram uses various symbols like circles, rectangles, and arrows to represent different entities and their interactions.

The diagram shows a floppy disk 2220 with six data blocks arranged in two columns. Each block is a rectangle with its address and content inside, and a pointer line connecting it to the disk's outer edge.

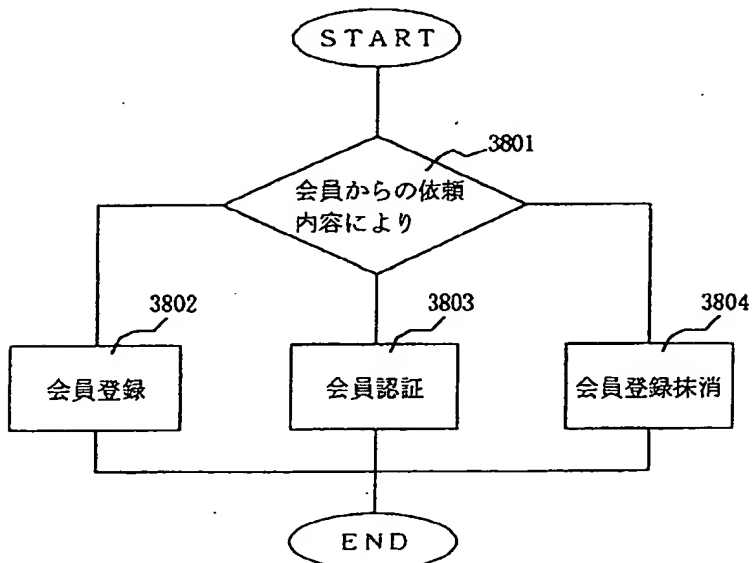
Address	Content
2500	暗号化秘密鍵
2501	ユーザ ID
2502	パスワード チェック用データ
2503	暗号化公開鍵
2504	暗号化自証明書
2505	認証機関証明書
2506	フロッピー ディスク番号

フロッピーディスク 2220

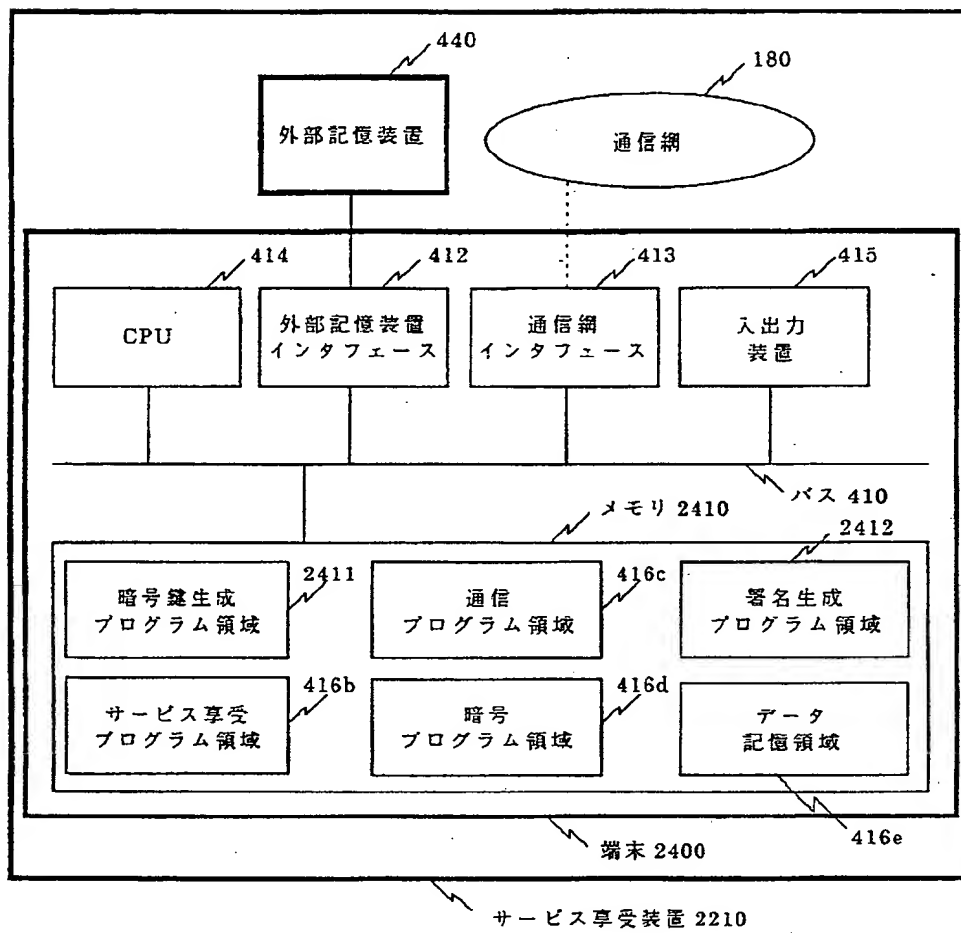
【図25】



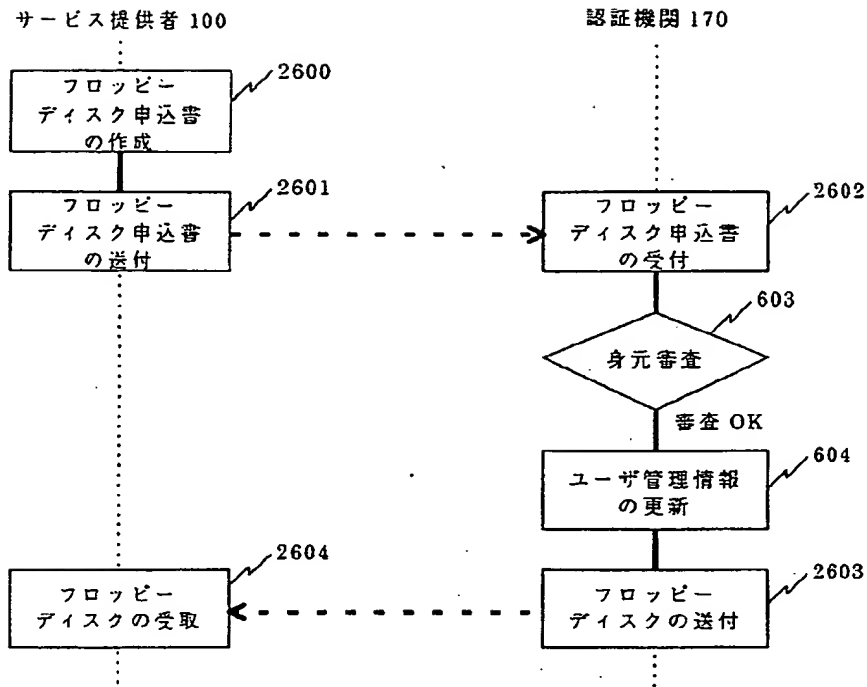
【図38】



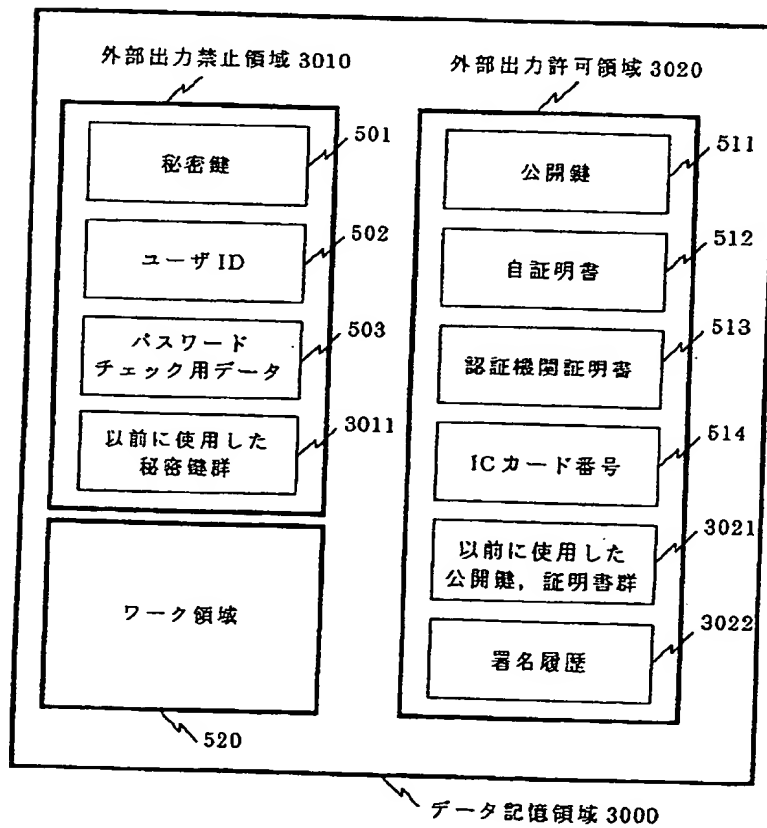
【図26】



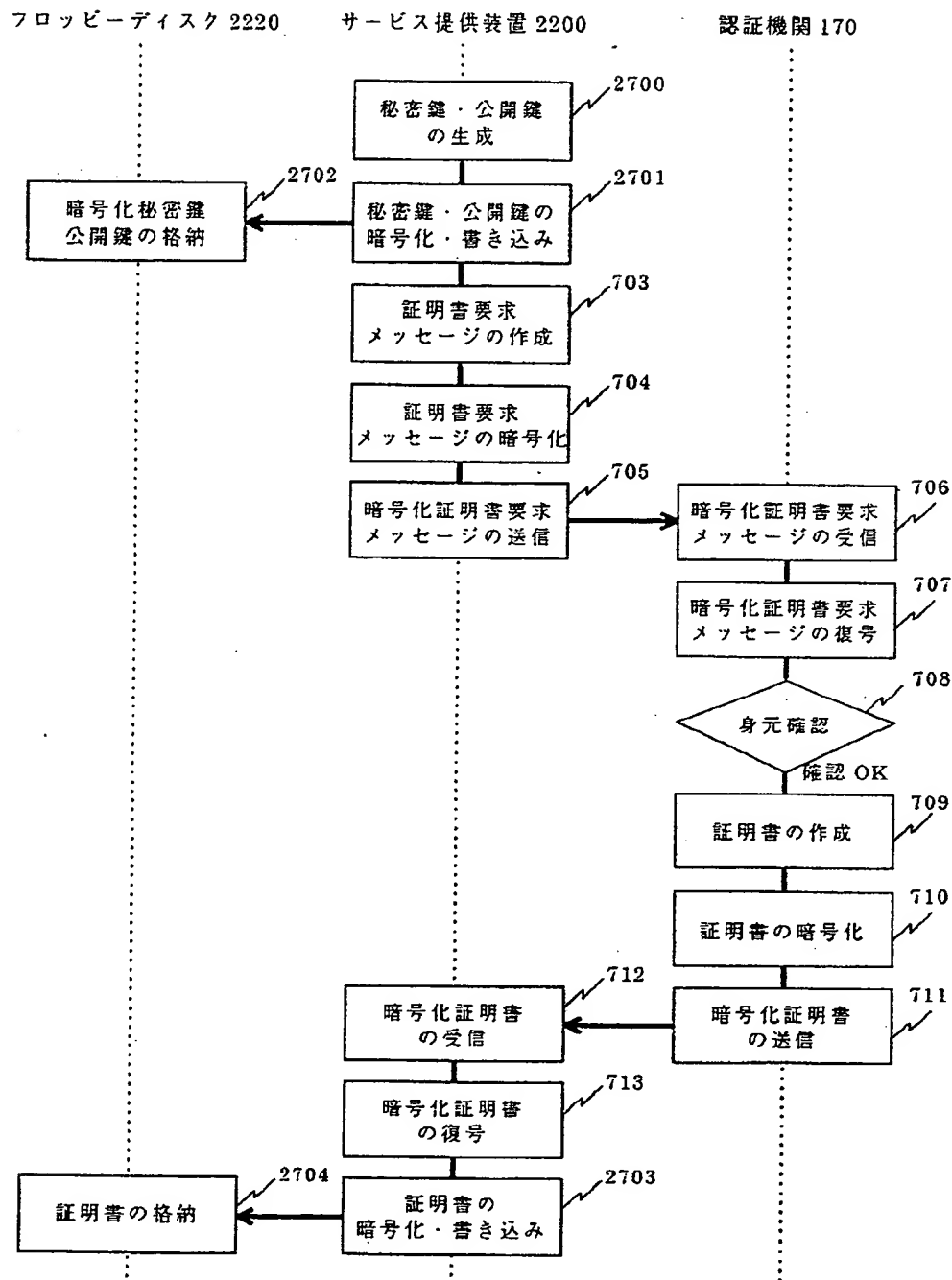
【図28】



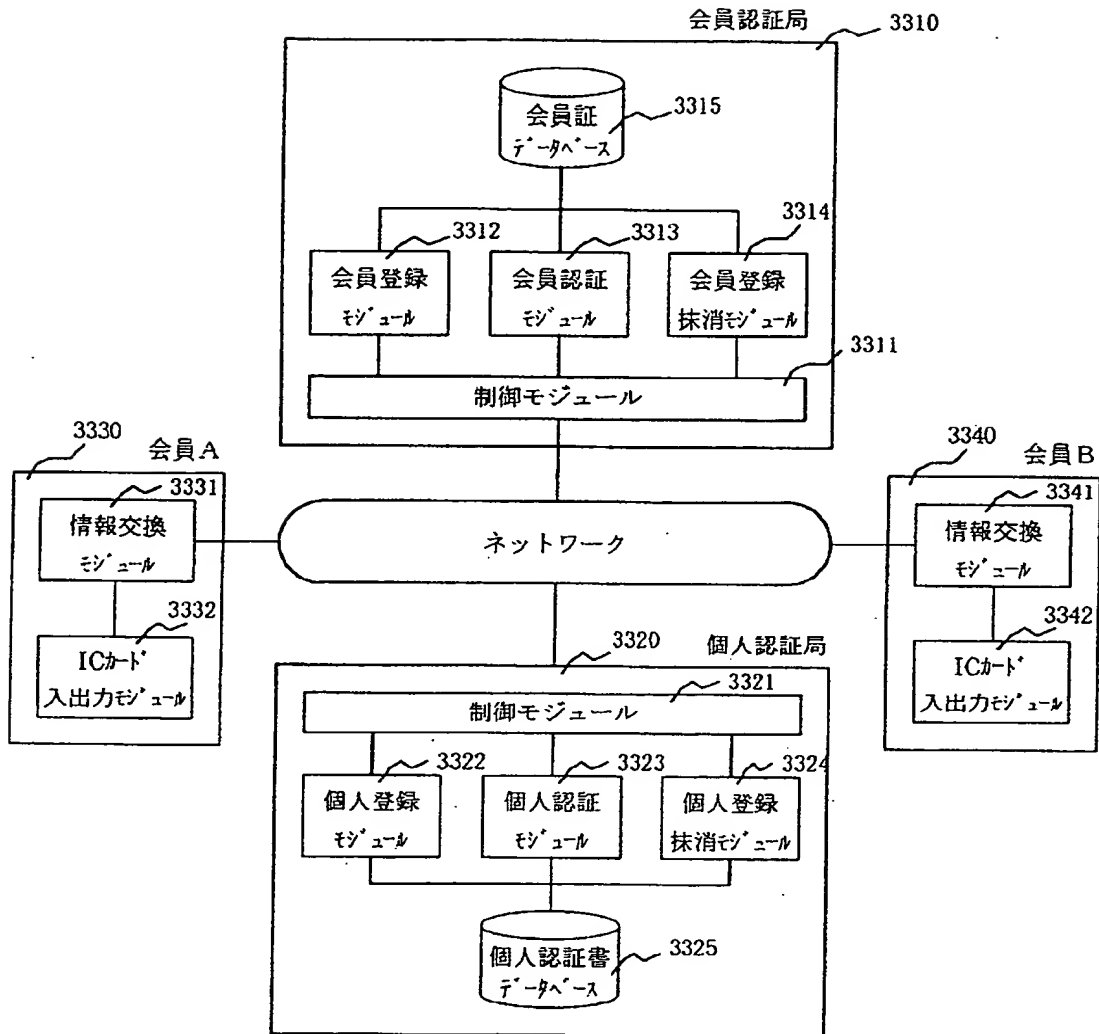
【図32】



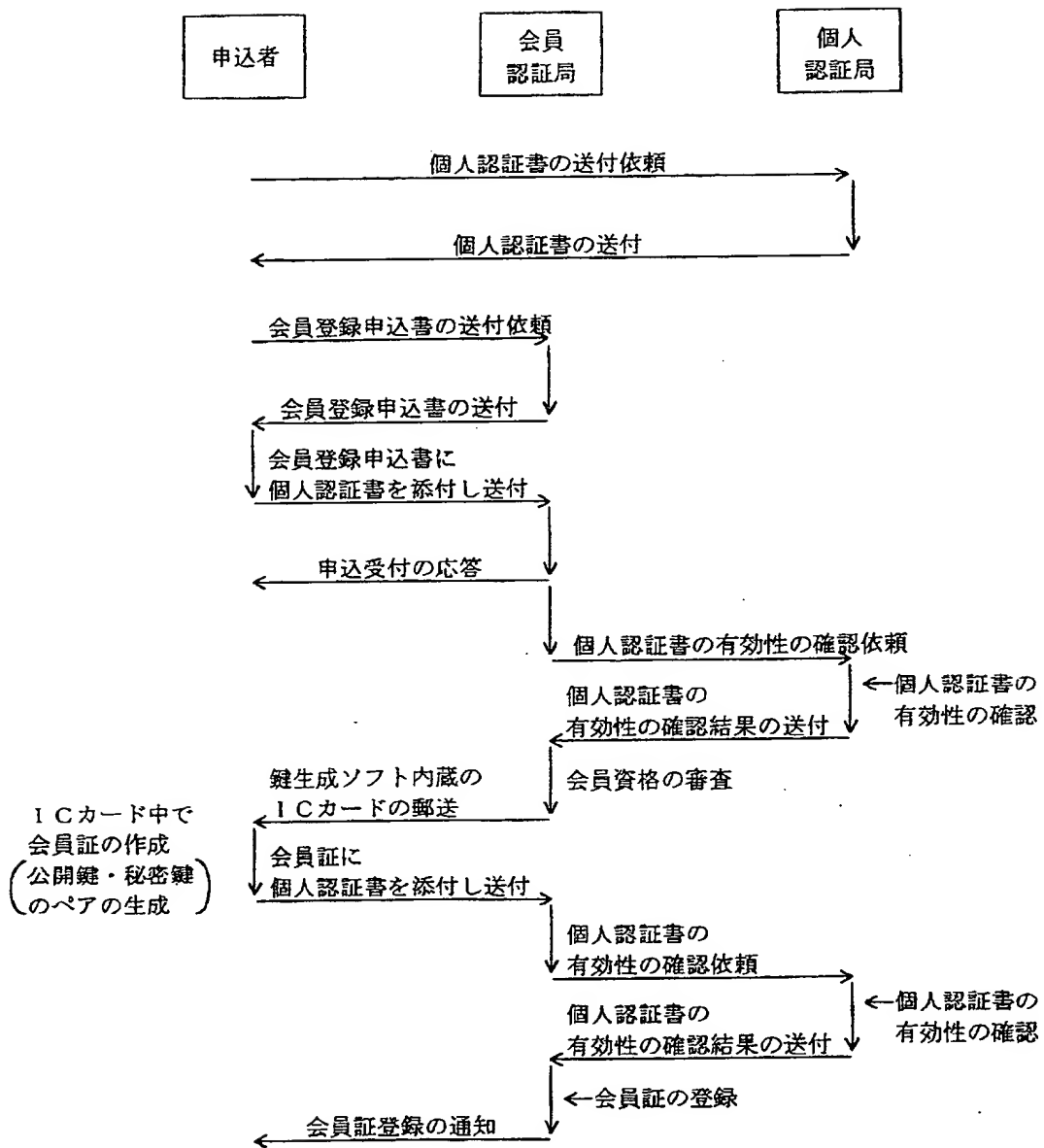
【図29】



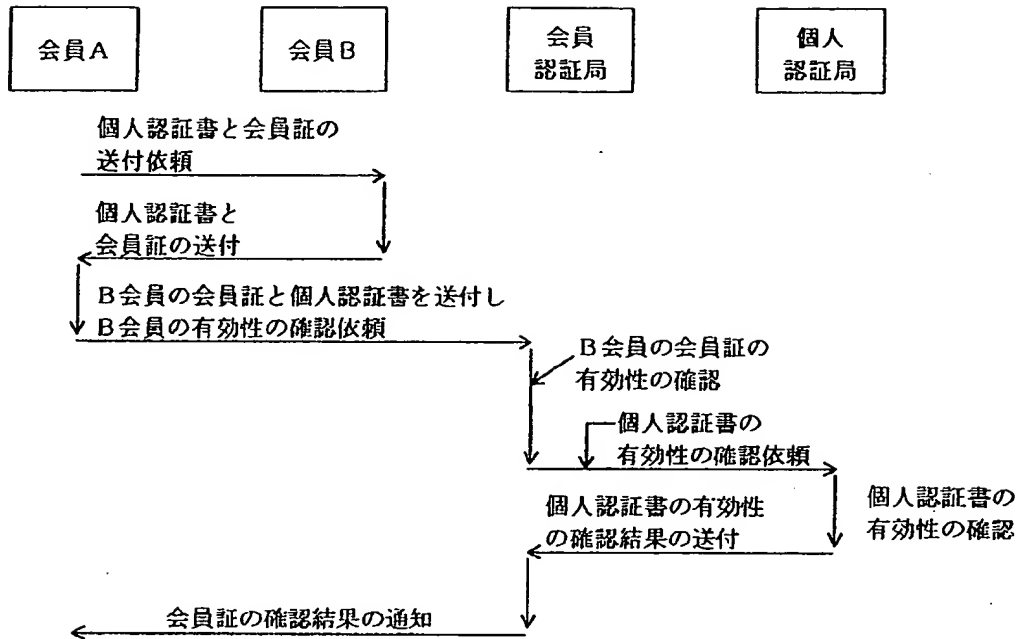
【図33】



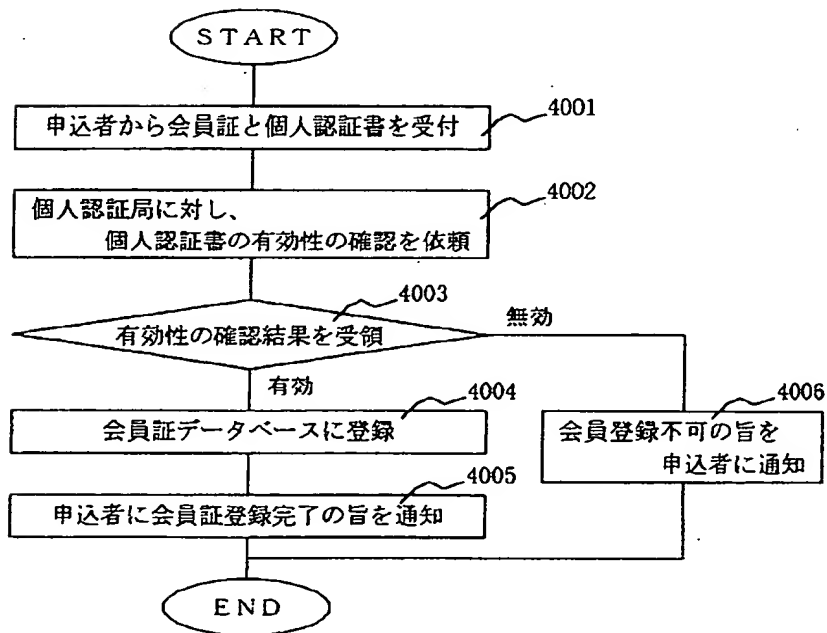
【図35】



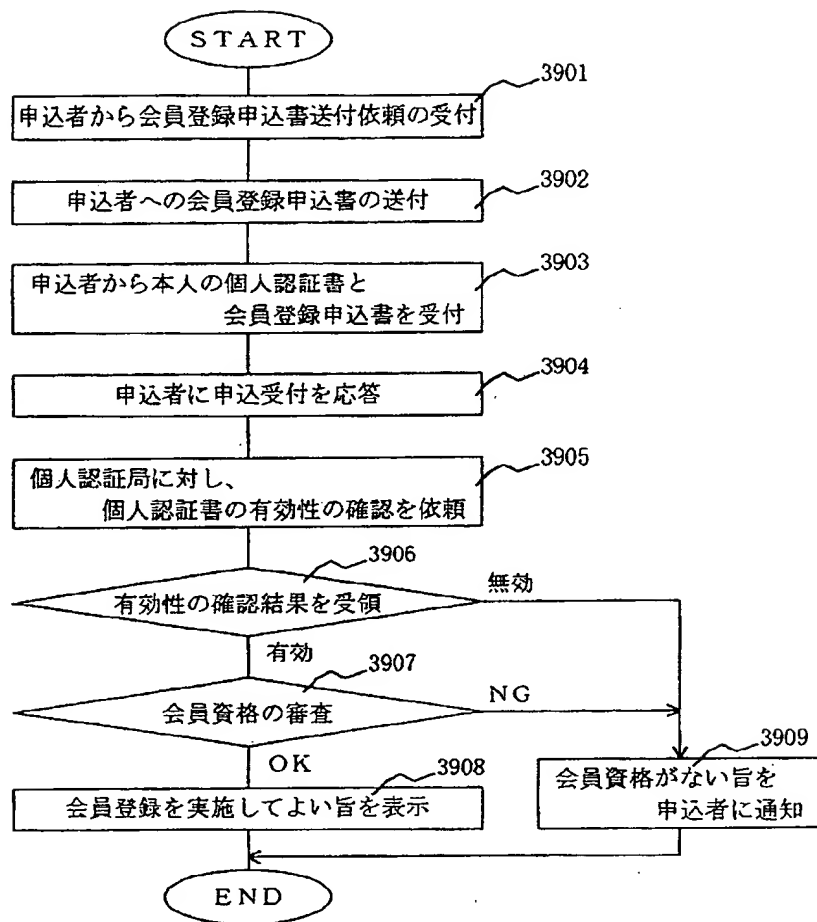
【図37】



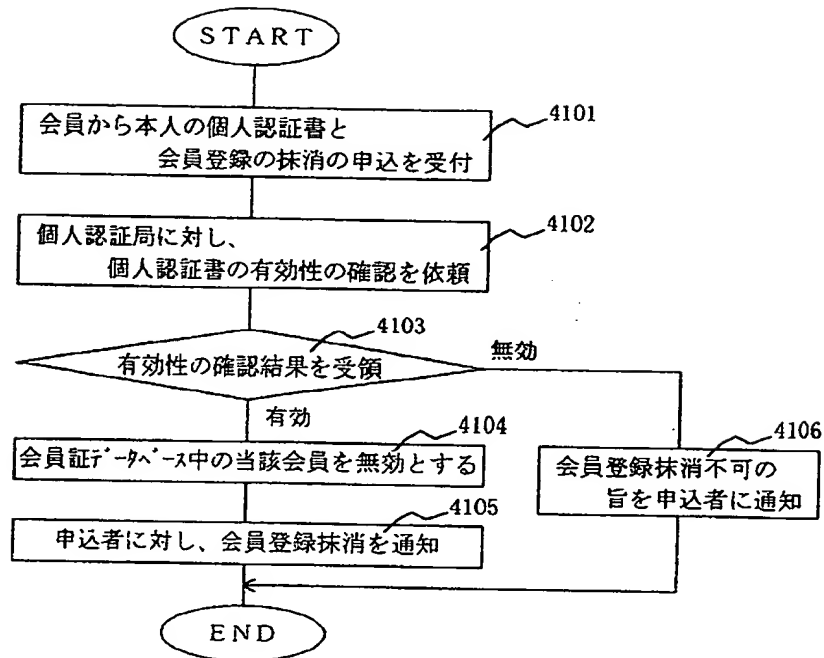
【図40】



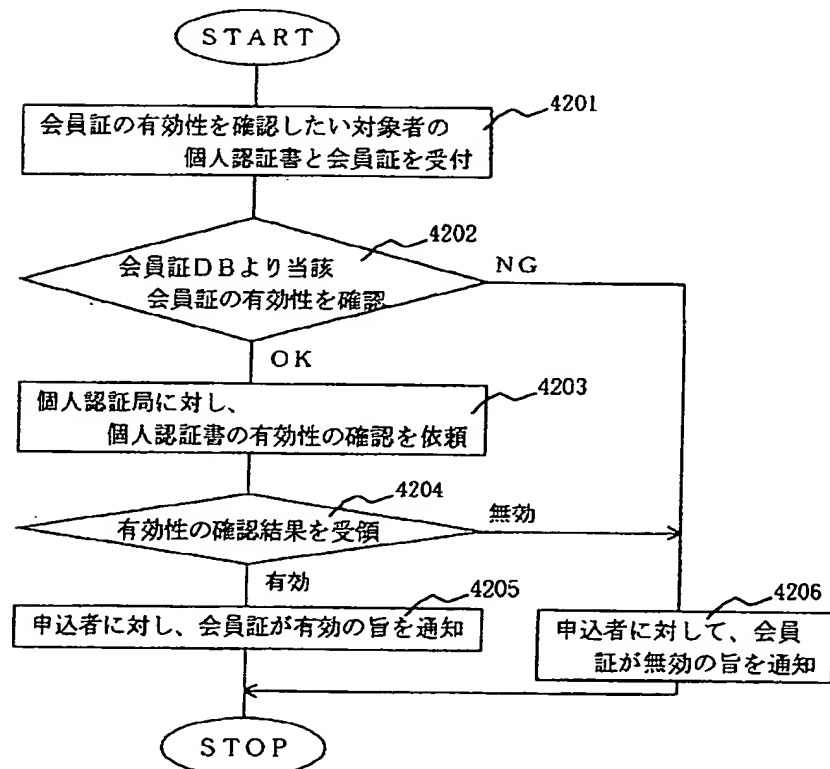
【図39】



【図41】

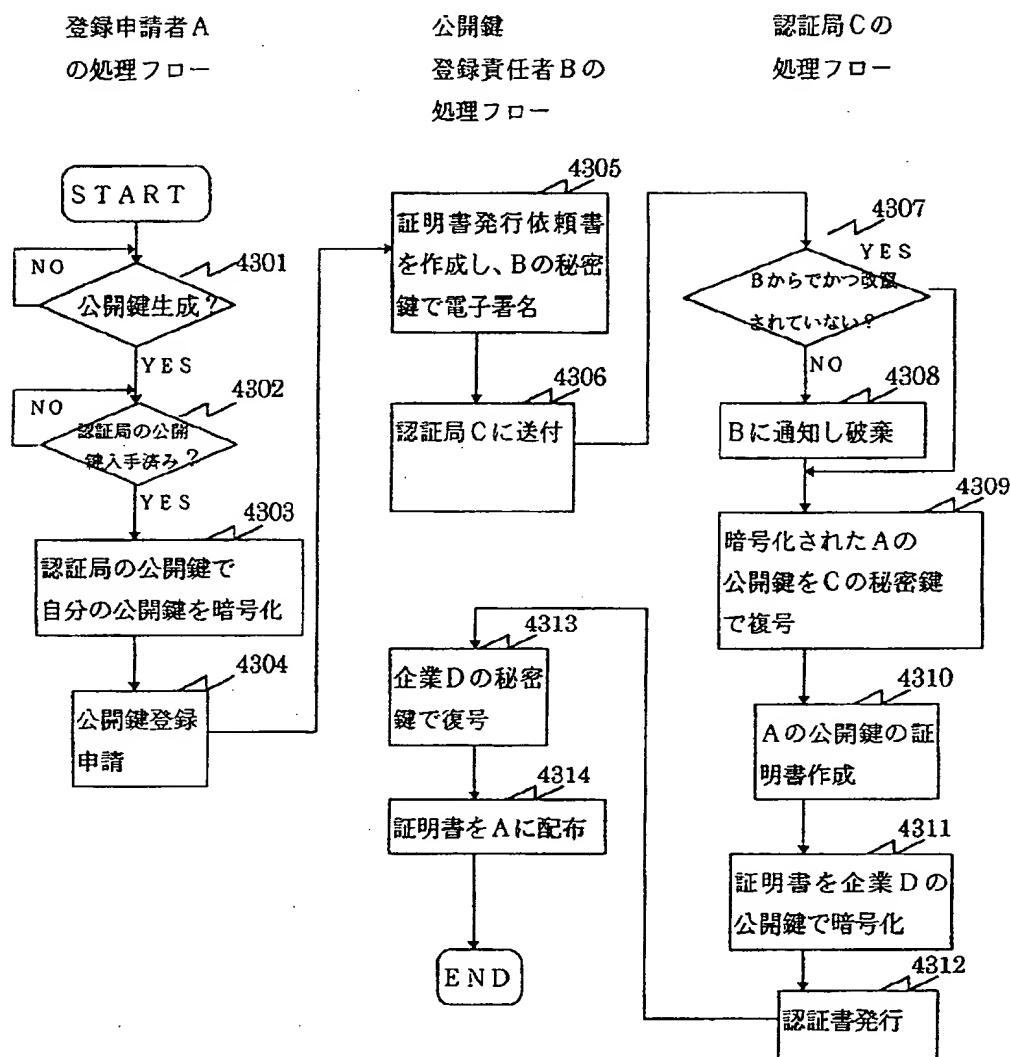


【図42】



【図43】

企業内認証における公開鍵登録の処理フロー



フロントページの続き

(72)発明者 高橋 美和
神奈川県川崎市幸区鹿島田890番地 株式
会社日立製作所ビジネスシステム開発セン
タ内

(72)発明者 光永 聖
神奈川県川崎市幸区鹿島田890番地 株式
会社日立製作所情報システム事業部内
(72)発明者 森山 将治
神奈川県川崎市幸区鹿島田890番地 株式
会社日立製作所情報システム事業部内